

BSI IT-Grundschutz A.1 Strukturanalyse

Informationsverbund:	Informationsverbund
Abkürzung:	SWDS
Mitarbeiter:	35
Geltungsbereich:	Kompletter Standort der Werft
Datum:	23.01.2024, 22:07
Autor:	Gruppe 4
Version:	0.1
Freigabe:	Sebastian Breu
Vorgehensweise der Absicherung:	STANDARD

Geschäftsprozesse

Kürzel	Name	Beschreibung	Prozess-Art
GP01	Konstruktion	Prozess der Erstellung, Revision und Ausarbeitung der digitalen Konzeption des Bauplans von Schiffen.	Unterstützender Prozess
	Mitarbeiter:	Entwicklung	
GP02	Einkauf	Prozess der Materialbeschaffung für die Konstruktion und Wartung von Schiffen	Unterstützender Prozess
	Mitarbeiter:	Einkauf	
GP03	Auftragsannahme / Verkauf	Prozess der Auftragsbearbeitung.	Unterstützender Prozess
	Mitarbeiter:	Vertrieb	
GP04	Fertigung	Prozess der Bau und Wartung von Schiffen.	Kerngeschäft
	Mitarbeiter:	Produktion	
GP05	Technischer Support	Der Prozess für die Bereitstellung von technischer Unterstützung und Lösungen Software, Hardware oder anderen IT-bezogenen Fragen.	Unterstützender Prozess
	Mitarbeiter:	IT-Betrieb, IT-Sicherheitsbeauftragter	

Anwendungen

Kürzel	Name	Beschreibung	Plattform / Baustein	Anzahl	Status
A01	Excel	Excel ermöglicht es den Mitarbeitern, umfangreiche Datenmengen aus Produktion und Vertrieb zu verarbeiten, zu analysieren und zu präsentieren. Excel wird für die Erstellung von Produktionsplänen, Verkaufsprognosen und Budgets genutzt.	MS Windows/APP.1.1	29	Betrieb
	Benutzer:	Produktion, Vertrieb			
A02	Outlook	Outlook ermöglicht es den Mitarbeitern, E-Mails zu senden und zu empfangen, wodurch die interne und externe Kommunikation erleichtert wird.	MS Windows/APP.5.2	29	Betrieb
	Benutzer:	Produktion, Vertrieb			
A03	Delftship	Delftship ist eine hochentwickelte Software für den Schiffsbau, die unseren Mitarbeitern eine umfassende Plattform für die digitale Konzeption von Schiffsauplänen bietet.	MS Windows/APP.7	11	Betrieb
	Benutzer:	Produktion			
A04	TeamViewer	Die Software ermöglicht es Benutzern, auf sichere Weise von verschiedenen Standorten aus auf Computer und andere Geräte zuzugreifen.	MS Windows/APP.3.1	29	Betrieb
	Benutzer:	Produktion, Vertrieb			
A05	Word	Microsoft Word ist eine weit verbreitete Textverarbeitungssoftware, die von den Abteilungen Produktion und Vertrieb in unserem Unternehmen genutzt wird.	MS Windows/APP.1.1	18	Betrieb
	Benutzer:	Vertrieb			

IT-Systeme

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
AP1	WLAN Access Point Produktion		7	Betrieb	Linux
	Benutzer:				
AP2	WLAN Access Point Betrieb		3	Betrieb	Linux

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
	Benutzer:				
C1	Client Betrieb APC		5	Betrieb	MS Windows
	Benutzer:	Einkauf, IT-Betrieb, Vertrieb			
C1	Client Betrieb Laptop		7	Betrieb	MS Windows
	Benutzer:	Einkauf, IT-Betrieb, Vertrieb			
C2	Client Produktion		3	Betrieb	MS Windows
	Benutzer:	Produktion			
C3	Client Produktionsleiter		6	Betrieb	iPadOS
	Benutzer:	Produktion			
C4	Client Sekretär		1	Betrieb	macOS, iPadOS
	Benutzer:	Helpdesk			
C5	Client Geschäftsführung		2	Betrieb	macOS, iPadOS
	Benutzer:	Behörden-/Unternehmensleitung			
C6	Client CNC Fräse		1	Betrieb	MS Windows
	Benutzer:	Produktion			
C7	Client Gussmaschine		1	Betrieb	MS Windows
	Benutzer:	Produktion			
D1	Drucker Betrieb		1	Betrieb	UNIX-Based
	Benutzer:	Vertrieb, IT-Betrieb			
D2	Drucker Produktion		1	Betrieb	UNIX-Based
	Benutzer:	Produktion			
HP1	Switch Betrieb		2	Betrieb	ARM9E
	Benutzer:	IT-Betrieb, Einkauf, Vertrieb			
HP2	Switch Produktion		1	Betrieb	ARM9E
	Benutzer:	Entwicklung, Produktion			
N1	Firewall Betrieb		1	Betrieb	ZLD4.60
	Benutzer:				
N2	Firewall Produktion		1	Betrieb	ZLD4.60
	Benutzer:				
R1	Router		1	Betrieb	LCOS

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
	Benutzer:				
S1	Server Betrieb		1	Betrieb	MS Windows
	Benutzer:				
S2	Server Produktion		1	Betrieb	MS Windows
	Benutzer:				

ICS-Systeme

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
S100	SPS	Die SPS spielt eine entscheidende Rolle bei der Überwachung und Steuerung von Maschinen, Förderbändern und anderen produktionsrelevanten Abläufen.	1	Betrieb	SPS
	Benutzer:	Produktion			
S101	Produktionsmaschine - CNC Fräse	Die CNC Fräse wird für die Herstellung von präzisen Bauteilen und Werkstücken aus verschiedenen Materialien wie Metall, Kunststoff oder Holz benutzt.	1	Betrieb	MS Windows
	Benutzer:	Produktion			
S102	Produktionsmaschine - Gussmaschine		1	Betrieb	MS Windows
	Benutzer:	Produktion			

Anderes/IOT-Systeme

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
I1	Videoüberwachung		17	Betrieb	MS Windows, Linux
	Benutzer:	Pförtner			
K1	Kaffeemaschine		1	Betrieb	UNIX-Based
	Benutzer:	Alle Mitarbeiter			

Kommunikationsverbindungen

Kürzel	Name	Erläuterung	Status	Plattform
AP1<>>N1	WLAN AP Betrieb<>>Firewall Betrieb		Betrieb	
	Benutzer:			
AP2<>>N2	WLAN AP Produktion<>>Firewall Produktion		Betrieb	
	Benutzer:			
C1/4/5<>>AP2	Client Betrieb<>>WLAN AP Betrieb		Betrieb	
	Benutzer:	IT-Betrieb, Behörden-/Unternehmensleitung, Einkauf, Human Resources, Helpdesk, Vertrieb		
C1/4/5<>>N1	Client Betrieb<>>Firewall Betrieb		Betrieb	
	Benutzer:	IT-Betrieb, Behörden-/Unternehmensleitung, Einkauf, Vertrieb, Helpdesk		
C1<>>C2	Client Betrieb<>>Client Produktion		Betrieb	
	Benutzer:	Produktion, IT-Betrieb, Einkauf, Vertrieb, Human Resources		
C1<>>C4	Client Betrieb<>>Client Sekretär		Betrieb	
	Benutzer:	Einkauf, Helpdesk, Vertrieb, IT-Betrieb, Human Resources		
C1<>>C5	Client Betrieb<>>Client Geschäftsführung		Betrieb	
	Benutzer:	IT-Betrieb, Behörden-/Unternehmensleitung, Einkauf, Vertrieb, Human Resources		
C1<>>D1	Client Betrieb<>>Drucker Betrieb		Betrieb	
	Benutzer:	IT-Betrieb, Einkauf, Vertrieb		
C1<>>S1	Client Betrieb<>>Server Betrieb		Betrieb	
	Benutzer:	IT-Betrieb, Einkauf, Vertrieb, Human Resources, Helpdesk		
C2/3/6/7<>>AP1	Client Produktion<>>WLAN AP Produktion		Betrieb	
	Benutzer:	Produktion		
C2/3<>>S100/ S101/102	Client Produktion/Produktionsleiter<>>ICS-Systeme		Betrieb	
	Benutzer:	Produktion		
C2/C3/C6/C7<>>N2	Client Produktion<>>Firewall Produktion		Betrieb	
	Benutzer:	Produktion		
C2<>>C3	Client Produktion<>>Client Produktionsleiter		Betrieb	
	Benutzer:	Produktion		

Kürzel	Name	Erläuterung	Status	Plattform
C2<→C6	Client Produktion<→Client CNC Fräse		Betrieb	
	Benutzer:	Produktion		
C2<→C7	Client Produktion<→Client Gussmaschine		Betrieb	
	Benutzer:	Produktion		
C2<→D2	Client Produktion<→Drucker Produktion		Betrieb	
	Benutzer:	Produktion		
C2<→S2	Client Produktion<→Server Produktion		Betrieb	
	Benutzer:	Produktion		
C3<→D2	Client Produktionsleiter<→Drucker Produktion		Betrieb	
	Benutzer:	Produktion		
C4<→C5	Client Sekretär<→Client Geschäftsführung		Betrieb	
	Benutzer:	Behörden-/Unternehmensleitung, Helpdesk		
C4<→D1	Client Sekräter<→Drucker Betrieb		Betrieb	
	Benutzer:	Helpdesk		
C5<→D1	Client Geschäftsführung<→Drucker Betrieb		Betrieb	
	Benutzer:	Behörden-/Unternehmensleitung		
HP1<→AP2	Switch Betrieb<→WLAN AP Betrieb		Betrieb	
	Benutzer:	IT-Betrieb, Einkauf, Vertrieb		
HP1<→C1/4/5	Switch Betrieb<→Client Betrieb		Betrieb	
	Benutzer:			
HP1<→D1	Switch Betrieb<→Drucker Betrieb		Betrieb	
	Benutzer:			
HP1<→N1	Server Betrieb<→Firewall Betrieb		Betrieb	
	Benutzer:			
HP1<→S1	Switch Betrieb<→Server Betrieb		Betrieb	
	Benutzer:			

Kürzel	Name	Erläuterung	Status	Plattform
HP2<>AP1	Switch Produktion<>WLAN AP Produktion		Betrieb	
	Benutzer:	Produktion, Entwicklung		
HP2<>C2/3	Switch Produktion<>Client Produktion		Betrieb	
	Benutzer:			
HP2<>N2	Switch Betrieb<>Firewall Betrieb		Betrieb	
	Benutzer:			
HP2<>S2	Switch Produktion<>Drucker Produktion		Betrieb	
	Benutzer:			
HP2<>S2	Switch Produktion<>Server Produktion		Betrieb	
	Benutzer:			
K40	Firewall Prod <> Router		Betrieb	
	Benutzer:			
K42	Router<>Videoüberwachung		Betrieb	kritische Verbindung = Außenverbindung
	Benutzer:			
K43	Router<>Internet		Betrieb	kritische Verbindung = Außenverbindung
	Benutzer:			
K44	Kaffeemaschine <> WLAN AP PROD		Betrieb	
	Benutzer:			
K45	Firewall Betrieb<>Router		Betrieb	
	Benutzer:			
K46	Firewall Betrieb<>Firewall Produktion		Betrieb	
	Benutzer:			
S1<>N1	Server Betrieb<>Firewall Betrieb		Betrieb	
	Benutzer:			
S1<>S2	Server Betrieb<>Server Produktion		Betrieb	
	Benutzer:			
S2<>N2	Server Produktion<>Firewall Produktion		Betrieb	

Kürzel	Name	Erläuterung	Status	Plattform
	Benutzer:			

Räume

Kürzel	Name	Erläuterung	Anzahl	Plattform
	Halle und Materiallager		1	
	Benutzer:	Produktion		
EG-1	Büroraum Geschäftsleiter		1	
	Benutzer:	Behörden-/Unternehmensleitung		
EG-2	Büroraum Personal		1	
	Benutzer:	Human Resources		
EG-3	Büroraum Entwicklung		1	
	Benutzer:	Entwicklung		
EG-4	Büroraum Einkauf		1	
	Benutzer:	Einkauf		
EG-5	Empfang/Wartebereich		1	
	Benutzer:	Helpdesk		
EG-6	Küche		1	
	Benutzer:	Alle Mitarbeiter		
LG-1	Büroraum Produktion		1	
	Benutzer:	Produktion		
LG-2	Küche		1	
	Benutzer:	Produktion		
OG-1	Büroraum Vertrieb		1	
	Benutzer:	Vertrieb		
OG-2	Büroraum IT Admin		1	
	Benutzer:	Administration		
OG-3	Büroraum CISO		1	
	Benutzer:	IT-Sicherheitsbeauftragter		
OG-4	Pausenraum		1	
	Benutzer:	Alle Mitarbeiter		

Kürzel	Name	Erläuterung	Anzahl	Plattform
OG-5	Serverraum		1	
	Benutzer:	IT-Betrieb, Administration, IT-Sicherheitsbeauftragter		

BSI IT-Grundschutz: A.1 Strukturanalyse-Abhängigkeiten

Informationsverbund:	Informationsverbund
Abkürzung:	SWDS
Mitarbeiter:	35
Geltungsbereich:	Kompletter Standort der Werft
Datum:	23.01.2024, 22:12
Autor:	Gruppe 4
Version:	0.1
Freigabe:	Sebastian Breu
Vorgehensweise der Absicherung:	STANDARD

Geschäftsprozesse

Kürzel	Name	Kürzel	Name
GP01	Konstruktion	Zuordnung	Kürzel
		benötigt	A02
		benötigt	A03
		benötigt	A04
		benötigt	A05
		benötigt	C2
		benötigt	C3
		benötigt	N2
		benötigt	R1
		benötigt	S2
		benötigt	K40
		Verantwortlicher	Mia Lindenberg
GP02	Einkauf	Zuordnung	Kürzel
		benötigt	A01
			Excel

Kürzel	Name		
GP02	Einkauf		
	<i>Zuordnung</i>		
	benötigt	Kürzel	Name
	benötigt	A02	Outlook
	benötigt	A04	TeamViewer
	benötigt	A05	Word
	benötigt	C1	Client Betrieb APC
	benötigt	C1	Client Betrieb Laptop
	benötigt	D1	Drucker Betrieb
	benötigt	N1	Firewall Betrieb
	benötigt	R1	Router
	benötigt	S1	Server Betrieb
	benötigt	C1/4/5↔N1	Client Betrieb↔Firewall Betrieb
	benötigt	K45	Firewall Betrieb<->Router
	Verantwortlicher		Heinrich Henckel von Donnersmarck
GP03	Auftragsannahme / Verkauf		
	<i>Zuordnung</i>		
	benötigt	Kürzel	Name
	benötigt	A01	Excel
	benötigt	A02	Outlook
	benötigt	A04	TeamViewer
	benötigt	A05	Word
	benötigt	C1	Client Betrieb APC
	benötigt	C1	Client Betrieb Laptop
	benötigt	C4	Client Sekretär
	benötigt	D1	Drucker Betrieb
	benötigt	N1	Firewall Betrieb
	benötigt	R1	Router
	benötigt	S1	Server Betrieb
	benötigt	C1/4/5↔N1	Client Betrieb↔Firewall Betrieb
	benötigt	K45	Firewall Betrieb<->Router
	Verantwortlicher		Heinrich Henckel von Donnersmarck

Kürzel	Name		
GP04	Fertigung		
	Zuordnung		
	benötigt	Kürzel	Name
	benötigt	A01	Excel
	benötigt	A02	Outlook
	benötigt	A03	Delftship
	benötigt	A04	TeamViewer
	benötigt	A05	Word
	benötigt	C2	Client Produktion
	benötigt	C3	Client Produktionsleiter
	benötigt	C6	Client CNC Fräse
	benötigt	C7	Client Gussmaschine
	benötigt	N2	Firewall Produktion
	benötigt	R1	Router
	benötigt	S2	Server Produktion
	benötigt	S100	SPS
	benötigt	S101	Produktionsmaschine - CNC Fräse
	benötigt	S102	Produktionsmaschine - Gussmaschine
	benötigt	K40	Firewall Prod <→ Router
	Verantwortlicher		Sylvia Gradl
GP05	Technischer Support		
	Zuordnung		
	benötigt	Kürzel	Name
	benötigt	A01	Excel
	benötigt	A04	TeamViewer
	benötigt	A05	Word
	benötigt	C1	Client Betrieb APC
	benötigt	C1	Client Betrieb Laptop
	benötigt	N1	Firewall Betrieb
	benötigt	R1	Router
	benötigt	S1	Server Betrieb
	benötigt	C1/4/5<→N1	Client Betrieb<→Firewall Betrieb
	benötigt	K45	Firewall Betrieb<->Router
	Verantwortlicher	Admin	Sebastian Breu

Anwendungen

Kürzel	Name																																																			
A01	Excel																																																			
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP02</td> <td>Einkauf</td> </tr> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td> </tr> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td> </tr> <tr> <td>nötig für</td> <td>GP05</td> <td>Technischer Support</td> </tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td> </tr> <tr> <td>benötigt</td> <td>C1</td> <td>Client Betrieb APC</td> </tr> <tr> <td>benötigt</td> <td>C1</td> <td>Client Betrieb Laptop</td> </tr> <tr> <td>benötigt</td> <td>C2</td> <td>Client Produktion</td> </tr> <tr> <td>benötigt</td> <td>C3</td> <td>Client Produktionsleiter</td> </tr> <tr> <td>benötigt</td> <td>C4</td> <td>Client Sekretär</td> </tr> <tr> <td>benötigt</td> <td>C5</td> <td>Client Geschäftsführung</td> </tr> <tr> <td>benötigt</td> <td>C6</td> <td>Client CNC Fräse</td> </tr> <tr> <td>benötigt</td> <td>C7</td> <td>Client Gussmaschine</td> </tr> <tr> <td>benötigt</td> <td>S1</td> <td>Server Betrieb</td> </tr> <tr> <td>benötigt</td> <td>S2</td> <td>Server Produktion</td> </tr> <tr> <td>Benutzer</td> <td>Admin</td> <td>Sebastian Breu</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP02	Einkauf	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	GP04	Fertigung	nötig für	GP05	Technischer Support	nötig für	A04	TeamViewer	benötigt	C1	Client Betrieb APC	benötigt	C1	Client Betrieb Laptop	benötigt	C2	Client Produktion	benötigt	C3	Client Produktionsleiter	benötigt	C4	Client Sekretär	benötigt	C5	Client Geschäftsführung	benötigt	C6	Client CNC Fräse	benötigt	C7	Client Gussmaschine	benötigt	S1	Server Betrieb	benötigt	S2	Server Produktion	Benutzer	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																																																		
nötig für	GP02	Einkauf																																																		
nötig für	GP03	Auftragsannahme / Verkauf																																																		
nötig für	GP04	Fertigung																																																		
nötig für	GP05	Technischer Support																																																		
nötig für	A04	TeamViewer																																																		
benötigt	C1	Client Betrieb APC																																																		
benötigt	C1	Client Betrieb Laptop																																																		
benötigt	C2	Client Produktion																																																		
benötigt	C3	Client Produktionsleiter																																																		
benötigt	C4	Client Sekretär																																																		
benötigt	C5	Client Geschäftsführung																																																		
benötigt	C6	Client CNC Fräse																																																		
benötigt	C7	Client Gussmaschine																																																		
benötigt	S1	Server Betrieb																																																		
benötigt	S2	Server Produktion																																																		
Benutzer	Admin	Sebastian Breu																																																		
A02	Outlook																																																			
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP01</td> <td>Konstruktion</td> </tr> <tr> <td>nötig für</td> <td>GP02</td> <td>Einkauf</td> </tr> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td> </tr> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td> </tr> <tr> <td>benötigt</td> <td>C1</td> <td>Client Betrieb APC</td> </tr> <tr> <td>benötigt</td> <td>C1</td> <td>Client Betrieb Laptop</td> </tr> <tr> <td>benötigt</td> <td>C2</td> <td>Client Produktion</td> </tr> <tr> <td>benötigt</td> <td>C3</td> <td>Client Produktionsleiter</td> </tr> <tr> <td>benötigt</td> <td>C4</td> <td>Client Sekretär</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP01	Konstruktion	nötig für	GP02	Einkauf	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	GP04	Fertigung	benötigt	C1	Client Betrieb APC	benötigt	C1	Client Betrieb Laptop	benötigt	C2	Client Produktion	benötigt	C3	Client Produktionsleiter	benötigt	C4	Client Sekretär																					
Zuordnung	Kürzel	Name																																																		
nötig für	GP01	Konstruktion																																																		
nötig für	GP02	Einkauf																																																		
nötig für	GP03	Auftragsannahme / Verkauf																																																		
nötig für	GP04	Fertigung																																																		
benötigt	C1	Client Betrieb APC																																																		
benötigt	C1	Client Betrieb Laptop																																																		
benötigt	C2	Client Produktion																																																		
benötigt	C3	Client Produktionsleiter																																																		
benötigt	C4	Client Sekretär																																																		

Kürzel	Name																																	
A02	Outlook																																	
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>benötigt</td><td>C5</td><td>Client Geschäftsführung</td></tr> <tr> <td>benötigt</td><td>C6</td><td>Client CNC Fräse</td></tr> <tr> <td>benötigt</td><td>C7</td><td>Client Gussmaschine</td></tr> <tr> <td>benötigt</td><td>S1</td><td>Server Betrieb</td></tr> <tr> <td>benötigt</td><td>S2</td><td>Server Produktion</td></tr> <tr> <td>Verantwortlicher</td><td></td><td>Mia Lindenberg</td></tr> <tr> <td>Verantwortlicher</td><td>Admin</td><td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	benötigt	C5	Client Geschäftsführung	benötigt	C6	Client CNC Fräse	benötigt	C7	Client Gussmaschine	benötigt	S1	Server Betrieb	benötigt	S2	Server Produktion	Verantwortlicher		Mia Lindenberg	Verantwortlicher	Admin	Sebastian Breu									
Zuordnung	Kürzel	Name																																
benötigt	C5	Client Geschäftsführung																																
benötigt	C6	Client CNC Fräse																																
benötigt	C7	Client Gussmaschine																																
benötigt	S1	Server Betrieb																																
benötigt	S2	Server Produktion																																
Verantwortlicher		Mia Lindenberg																																
Verantwortlicher	Admin	Sebastian Breu																																
A03	Delftship																																	
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td><td>GP01</td><td>Konstruktion</td></tr> <tr> <td>nötig für</td><td>GP04</td><td>Fertigung</td></tr> <tr> <td>benötigt</td><td>C2</td><td>Client Produktion</td></tr> <tr> <td>benötigt</td><td>C3</td><td>Client Produktionsleiter</td></tr> <tr> <td>benötigt</td><td>C6</td><td>Client CNC Fräse</td></tr> <tr> <td>benötigt</td><td>C7</td><td>Client Gussmaschine</td></tr> <tr> <td>benötigt</td><td>S2</td><td>Server Produktion</td></tr> <tr> <td>Verantwortlicher</td><td></td><td>Mia Lindenberg</td></tr> <tr> <td>Verantwortlicher</td><td>Admin</td><td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP01	Konstruktion	nötig für	GP04	Fertigung	benötigt	C2	Client Produktion	benötigt	C3	Client Produktionsleiter	benötigt	C6	Client CNC Fräse	benötigt	C7	Client Gussmaschine	benötigt	S2	Server Produktion	Verantwortlicher		Mia Lindenberg	Verantwortlicher	Admin	Sebastian Breu			
Zuordnung	Kürzel	Name																																
nötig für	GP01	Konstruktion																																
nötig für	GP04	Fertigung																																
benötigt	C2	Client Produktion																																
benötigt	C3	Client Produktionsleiter																																
benötigt	C6	Client CNC Fräse																																
benötigt	C7	Client Gussmaschine																																
benötigt	S2	Server Produktion																																
Verantwortlicher		Mia Lindenberg																																
Verantwortlicher	Admin	Sebastian Breu																																
A04	TeamViewer																																	
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td><td>GP01</td><td>Konstruktion</td></tr> <tr> <td>nötig für</td><td>GP02</td><td>Einkauf</td></tr> <tr> <td>nötig für</td><td>GP03</td><td>Auftragsannahme / Verkauf</td></tr> <tr> <td>nötig für</td><td>GP04</td><td>Fertigung</td></tr> <tr> <td>nötig für</td><td>GP05</td><td>Technischer Support</td></tr> <tr> <td>benötigt</td><td>A01</td><td>Excel</td></tr> <tr> <td>benötigt</td><td>C1</td><td>Client Betrieb APC</td></tr> <tr> <td>benötigt</td><td>C1</td><td>Client Betrieb Laptop</td></tr> <tr> <td>benötigt</td><td>C2</td><td>Client Produktion</td></tr> <tr> <td>benötigt</td><td>C3</td><td>Client Produktionsleiter</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP01	Konstruktion	nötig für	GP02	Einkauf	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	GP04	Fertigung	nötig für	GP05	Technischer Support	benötigt	A01	Excel	benötigt	C1	Client Betrieb APC	benötigt	C1	Client Betrieb Laptop	benötigt	C2	Client Produktion	benötigt	C3	Client Produktionsleiter
Zuordnung	Kürzel	Name																																
nötig für	GP01	Konstruktion																																
nötig für	GP02	Einkauf																																
nötig für	GP03	Auftragsannahme / Verkauf																																
nötig für	GP04	Fertigung																																
nötig für	GP05	Technischer Support																																
benötigt	A01	Excel																																
benötigt	C1	Client Betrieb APC																																
benötigt	C1	Client Betrieb Laptop																																
benötigt	C2	Client Produktion																																
benötigt	C3	Client Produktionsleiter																																

Kürzel	Name		
A04	TeamViewer		
	Zuordnung	Kürzel	Name
	benötigt	C4	Client Sekretär
	benötigt	C5	Client Geschäftsführung
	benötigt	C6	Client CNC Fräse
	benötigt	C7	Client Gussmaschine
	benötigt	S1	Server Betrieb
	benötigt	S2	Server Produktion
	Benutzer	Admin	Sebastian Breu
A05	Word		
	Zuordnung	Kürzel	Name
	nötig für	GP01	Konstruktion
	nötig für	GP02	Einkauf
	nötig für	GP03	Auftragsannahme / Verkauf
	nötig für	GP04	Fertigung
	nötig für	GP05	Technischer Support
	benötigt	C1	Client Betrieb APC
	benötigt	C1	Client Betrieb Laptop
	benötigt	C4	Client Sekretär
	benötigt	C5	Client Geschäftsführung
	benötigt	S1	Server Betrieb
	Benutzer	Admin	Sebastian Breu

IT-System

Kürzel	Name		
AP1	WLAN Access Point Produktion		
	Zuordnung	Kürzel	Name
	benötigt	HP2	Switch Produktion
	benötigt	N2	Firewall Produktion
	benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion
	benötigt	K44	Kaffeemaschine <> WLAN AP PROD

Kürzel	Name																																																												
AP1	WLAN Access Point Produktion																																																												
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	Administrator	Admin	Sebastian Breu																																																						
Zuordnung	Kürzel	Name																																																											
Administrator	Admin	Sebastian Breu																																																											
AP2	WLAN Access Point Betrieb																																																												
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>benötigt</td> <td>HP1</td> <td>Switch Betrieb</td> </tr> <tr> <td>benötigt</td> <td>N1</td> <td>Firewall Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C1/4/5<>AP2</td> <td>Client Betrieb<>WLAN AP Betrieb</td> </tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	benötigt	HP1	Switch Betrieb	benötigt	N1	Firewall Betrieb	benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb	Administrator	Admin	Sebastian Breu																																													
Zuordnung	Kürzel	Name																																																											
benötigt	HP1	Switch Betrieb																																																											
benötigt	N1	Firewall Betrieb																																																											
benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb																																																											
Administrator	Admin	Sebastian Breu																																																											
C1	Client Betrieb Laptop																																																												
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP02</td> <td>Einkauf</td> </tr> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td> </tr> <tr> <td>nötig für</td> <td>GP05</td> <td>Technischer Support</td> </tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td> </tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td> </tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td> </tr> <tr> <td>nötig für</td> <td>A05</td> <td>Word</td> </tr> <tr> <td>benötigt</td> <td>C1/4/5<>AP2</td> <td>Client Betrieb<>WLAN AP Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C1/4/5<>N1</td> <td>Client Betrieb<>Firewall Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C1<>C2</td> <td>Client Betrieb<>Client Produktion</td> </tr> <tr> <td>benötigt</td> <td>C1<>C4</td> <td>Client Betrieb<>Client Sekretär</td> </tr> <tr> <td>benötigt</td> <td>C1<>C5</td> <td>Client Betrieb<>Client Geschäftsführung</td> </tr> <tr> <td>benötigt</td> <td>C1<>D1</td> <td>Client Betrieb<>Drucker Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C1<>S1</td> <td>Client Betrieb<>Server Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C4<>C5</td> <td>Client Sekretär<>Client Geschäftsführung</td> </tr> <tr> <td>benötigt</td> <td>HP1<>C1/4/5</td> <td>Switch Betrieb<>Client Betrieb</td> </tr> <tr> <td>Anwender</td> <td></td> <td>Ulrike Schmidt</td> </tr> <tr> <td>Verantwortlicher</td> <td></td> <td>Heinrich Henckel von Donnersmarck</td> </tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP02	Einkauf	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	GP05	Technischer Support	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A04	TeamViewer	nötig für	A05	Word	benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb	benötigt	C1/4/5<>N1	Client Betrieb<>Firewall Betrieb	benötigt	C1<>C2	Client Betrieb<>Client Produktion	benötigt	C1<>C4	Client Betrieb<>Client Sekretär	benötigt	C1<>C5	Client Betrieb<>Client Geschäftsführung	benötigt	C1<>D1	Client Betrieb<>Drucker Betrieb	benötigt	C1<>S1	Client Betrieb<>Server Betrieb	benötigt	C4<>C5	Client Sekretär<>Client Geschäftsführung	benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb	Anwender		Ulrike Schmidt	Verantwortlicher		Heinrich Henckel von Donnersmarck	Administrator	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																																																											
nötig für	GP02	Einkauf																																																											
nötig für	GP03	Auftragsannahme / Verkauf																																																											
nötig für	GP05	Technischer Support																																																											
nötig für	A01	Excel																																																											
nötig für	A02	Outlook																																																											
nötig für	A04	TeamViewer																																																											
nötig für	A05	Word																																																											
benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb																																																											
benötigt	C1/4/5<>N1	Client Betrieb<>Firewall Betrieb																																																											
benötigt	C1<>C2	Client Betrieb<>Client Produktion																																																											
benötigt	C1<>C4	Client Betrieb<>Client Sekretär																																																											
benötigt	C1<>C5	Client Betrieb<>Client Geschäftsführung																																																											
benötigt	C1<>D1	Client Betrieb<>Drucker Betrieb																																																											
benötigt	C1<>S1	Client Betrieb<>Server Betrieb																																																											
benötigt	C4<>C5	Client Sekretär<>Client Geschäftsführung																																																											
benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb																																																											
Anwender		Ulrike Schmidt																																																											
Verantwortlicher		Heinrich Henckel von Donnersmarck																																																											
Administrator	Admin	Sebastian Breu																																																											

Kürzel	Name																																																												
C1	Client Betrieb APC																																																												
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP02</td> <td>Einkauf</td></tr> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td></tr> <tr> <td>nötig für</td> <td>GP05</td> <td>Technischer Support</td></tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td></tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td></tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td></tr> <tr> <td>nötig für</td> <td>A05</td> <td>Word</td></tr> <tr> <td>benötigt</td> <td>C1/4/5>AP2</td> <td>Client Betrieb<>WLAN AP Betrieb</td></tr> <tr> <td>benötigt</td> <td>C1/4/5>N1</td> <td>Client Betrieb<>Firewall Betrieb</td></tr> <tr> <td>benötigt</td> <td>C1>C2</td> <td>Client Betrieb<>Client Produktion</td></tr> <tr> <td>benötigt</td> <td>C1>C4</td> <td>Client Betrieb<>Client Sekretär</td></tr> <tr> <td>benötigt</td> <td>C1>C5</td> <td>Client Betrieb<>Client Geschäftsführung</td></tr> <tr> <td>benötigt</td> <td>C1>D1</td> <td>Client Betrieb<>Drucker Betrieb</td></tr> <tr> <td>benötigt</td> <td>C1>S1</td> <td>Client Betrieb<>Server Betrieb</td></tr> <tr> <td>benötigt</td> <td>C4>C5</td> <td>Client Sekretär<>Client Geschäftsführung</td></tr> <tr> <td>benötigt</td> <td>HP1>C1/4/5</td> <td>Switch Betrieb<>Client Betrieb</td></tr> <tr> <td>Anwender</td><td></td><td>Doris Richarz</td></tr> <tr> <td>Verantwortlicher</td><td></td><td>Lieselotte Hans</td></tr> <tr> <td>Administrator</td><td>Admin</td><td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP02	Einkauf	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	GP05	Technischer Support	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A04	TeamViewer	nötig für	A05	Word	benötigt	C1/4/5>AP2	Client Betrieb<>WLAN AP Betrieb	benötigt	C1/4/5>N1	Client Betrieb<>Firewall Betrieb	benötigt	C1>C2	Client Betrieb<>Client Produktion	benötigt	C1>C4	Client Betrieb<>Client Sekretär	benötigt	C1>C5	Client Betrieb<>Client Geschäftsführung	benötigt	C1>D1	Client Betrieb<>Drucker Betrieb	benötigt	C1>S1	Client Betrieb<>Server Betrieb	benötigt	C4>C5	Client Sekretär<>Client Geschäftsführung	benötigt	HP1>C1/4/5	Switch Betrieb<>Client Betrieb	Anwender		Doris Richarz	Verantwortlicher		Lieselotte Hans	Administrator	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																																																											
nötig für	GP02	Einkauf																																																											
nötig für	GP03	Auftragsannahme / Verkauf																																																											
nötig für	GP05	Technischer Support																																																											
nötig für	A01	Excel																																																											
nötig für	A02	Outlook																																																											
nötig für	A04	TeamViewer																																																											
nötig für	A05	Word																																																											
benötigt	C1/4/5>AP2	Client Betrieb<>WLAN AP Betrieb																																																											
benötigt	C1/4/5>N1	Client Betrieb<>Firewall Betrieb																																																											
benötigt	C1>C2	Client Betrieb<>Client Produktion																																																											
benötigt	C1>C4	Client Betrieb<>Client Sekretär																																																											
benötigt	C1>C5	Client Betrieb<>Client Geschäftsführung																																																											
benötigt	C1>D1	Client Betrieb<>Drucker Betrieb																																																											
benötigt	C1>S1	Client Betrieb<>Server Betrieb																																																											
benötigt	C4>C5	Client Sekretär<>Client Geschäftsführung																																																											
benötigt	HP1>C1/4/5	Switch Betrieb<>Client Betrieb																																																											
Anwender		Doris Richarz																																																											
Verantwortlicher		Lieselotte Hans																																																											
Administrator	Admin	Sebastian Breu																																																											
C2	Client Produktion																																																												
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP01</td> <td>Konstruktion</td></tr> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td></tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td></tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td></tr> <tr> <td>nötig für</td> <td>A03</td> <td>Delftship</td></tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td></tr> <tr> <td>benötigt</td> <td>D2</td> <td>Drucker Produktion</td></tr> <tr> <td>benötigt</td> <td>C1>C2</td> <td>Client Betrieb<>Client Produktion</td></tr> <tr> <td>benötigt</td> <td>C2/3/6/7>AP1</td> <td>Client Produktion<>WLAN AP Produktion</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP01	Konstruktion	nötig für	GP04	Fertigung	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A03	Delftship	nötig für	A04	TeamViewer	benötigt	D2	Drucker Produktion	benötigt	C1>C2	Client Betrieb<>Client Produktion	benötigt	C2/3/6/7>AP1	Client Produktion<>WLAN AP Produktion																														
Zuordnung	Kürzel	Name																																																											
nötig für	GP01	Konstruktion																																																											
nötig für	GP04	Fertigung																																																											
nötig für	A01	Excel																																																											
nötig für	A02	Outlook																																																											
nötig für	A03	Delftship																																																											
nötig für	A04	TeamViewer																																																											
benötigt	D2	Drucker Produktion																																																											
benötigt	C1>C2	Client Betrieb<>Client Produktion																																																											
benötigt	C2/3/6/7>AP1	Client Produktion<>WLAN AP Produktion																																																											

Kürzel	Name																																																
C2	Client Produktion																																																
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>benötigt</td><td>C2/3<>S100/S101/102</td><td>Client Produktion/Produktionsleiter<>ICS-Systeme</td></tr> <tr> <td>benötigt</td><td>C2/C3/C6/C7<>N2</td><td>Client Produktion<>Firewall Produktion</td></tr> <tr> <td>benötigt</td><td>C2<>C3</td><td>Client Produktion<>Client Produktionsleiter</td></tr> <tr> <td>benötigt</td><td>C2<>C6</td><td>Client Produktion<>Client CNC Fräse</td></tr> <tr> <td>benötigt</td><td>C2<>C7</td><td>Client Produktion<>Client Gussmaschine</td></tr> <tr> <td>benötigt</td><td>C2<>D2</td><td>Client Produktion<>Drucker Produktion</td></tr> <tr> <td>benötigt</td><td>C2<>S2</td><td>Client Produktion<>Server Produktion</td></tr> <tr> <td>benötigt</td><td>HP2<>C2/3</td><td>Switch Produktion<>Client Produktion</td></tr> <tr> <td>Anwender</td><td></td><td>Nicolas Traidl</td></tr> <tr> <td>Verantwortlicher</td><td></td><td>Mia Lindenberg</td></tr> <tr> <td>Administrator</td><td>Admin</td><td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme	benötigt	C2/C3/C6/C7<>N2	Client Produktion<>Firewall Produktion	benötigt	C2<>C3	Client Produktion<>Client Produktionsleiter	benötigt	C2<>C6	Client Produktion<>Client CNC Fräse	benötigt	C2<>C7	Client Produktion<>Client Gussmaschine	benötigt	C2<>D2	Client Produktion<>Drucker Produktion	benötigt	C2<>S2	Client Produktion<>Server Produktion	benötigt	HP2<>C2/3	Switch Produktion<>Client Produktion	Anwender		Nicolas Traidl	Verantwortlicher		Mia Lindenberg	Administrator	Admin	Sebastian Breu												
Zuordnung	Kürzel	Name																																															
benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme																																															
benötigt	C2/C3/C6/C7<>N2	Client Produktion<>Firewall Produktion																																															
benötigt	C2<>C3	Client Produktion<>Client Produktionsleiter																																															
benötigt	C2<>C6	Client Produktion<>Client CNC Fräse																																															
benötigt	C2<>C7	Client Produktion<>Client Gussmaschine																																															
benötigt	C2<>D2	Client Produktion<>Drucker Produktion																																															
benötigt	C2<>S2	Client Produktion<>Server Produktion																																															
benötigt	HP2<>C2/3	Switch Produktion<>Client Produktion																																															
Anwender		Nicolas Traidl																																															
Verantwortlicher		Mia Lindenberg																																															
Administrator	Admin	Sebastian Breu																																															
C3	Client Produktionsleiter																																																
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td><td>GP01</td><td>Konstruktion</td></tr> <tr> <td>nötig für</td><td>GP04</td><td>Fertigung</td></tr> <tr> <td>nötig für</td><td>A01</td><td>Excel</td></tr> <tr> <td>nötig für</td><td>A02</td><td>Outlook</td></tr> <tr> <td>nötig für</td><td>A03</td><td>Delftship</td></tr> <tr> <td>nötig für</td><td>A04</td><td>TeamViewer</td></tr> <tr> <td>benötigt</td><td>C2/3/6/7<>AP1</td><td>Client Produktion<>WLAN AP Produktion</td></tr> <tr> <td>benötigt</td><td>C2/3<>S100/S101/102</td><td>Client Produktion/Produktionsleiter<>ICS-Systeme</td></tr> <tr> <td>benötigt</td><td>C2/C3/C6/C7<>N2</td><td>Client Produktion<>Firewall Produktion</td></tr> <tr> <td>benötigt</td><td>C2<>C3</td><td>Client Produktion<>Client Produktionsleiter</td></tr> <tr> <td>benötigt</td><td>C2<>S2</td><td>Client Produktion<>Server Produktion</td></tr> <tr> <td>benötigt</td><td>C3<>D2</td><td>Client Produktionsleiter<>Drucker Produktion</td></tr> <tr> <td>benötigt</td><td>HP2<>C2/3</td><td>Switch Produktion<>Client Produktion</td></tr> <tr> <td>Verantwortlicher</td><td></td><td>Mia Lindenberg</td></tr> <tr> <td>Administrator</td><td>Admin</td><td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP01	Konstruktion	nötig für	GP04	Fertigung	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A03	Delftship	nötig für	A04	TeamViewer	benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion	benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme	benötigt	C2/C3/C6/C7<>N2	Client Produktion<>Firewall Produktion	benötigt	C2<>C3	Client Produktion<>Client Produktionsleiter	benötigt	C2<>S2	Client Produktion<>Server Produktion	benötigt	C3<>D2	Client Produktionsleiter<>Drucker Produktion	benötigt	HP2<>C2/3	Switch Produktion<>Client Produktion	Verantwortlicher		Mia Lindenberg	Administrator	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																																															
nötig für	GP01	Konstruktion																																															
nötig für	GP04	Fertigung																																															
nötig für	A01	Excel																																															
nötig für	A02	Outlook																																															
nötig für	A03	Delftship																																															
nötig für	A04	TeamViewer																																															
benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion																																															
benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme																																															
benötigt	C2/C3/C6/C7<>N2	Client Produktion<>Firewall Produktion																																															
benötigt	C2<>C3	Client Produktion<>Client Produktionsleiter																																															
benötigt	C2<>S2	Client Produktion<>Server Produktion																																															
benötigt	C3<>D2	Client Produktionsleiter<>Drucker Produktion																																															
benötigt	HP2<>C2/3	Switch Produktion<>Client Produktion																																															
Verantwortlicher		Mia Lindenberg																																															
Administrator	Admin	Sebastian Breu																																															

Kürzel	Name																																													
C4	Client Sekretär																																													
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td></tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td></tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td></tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td></tr> <tr> <td>nötig für</td> <td>A05</td> <td>Word</td></tr> <tr> <td>benötigt</td> <td>C1/4/5<>AP2</td> <td>Client Betrieb<>WLAN AP Betrieb</td></tr> <tr> <td>benötigt</td> <td>C1/4/5<>N1</td> <td>Client Betrieb<>Firewall Betrieb</td></tr> <tr> <td>benötigt</td> <td>C1<>C4</td> <td>Client Betrieb<>Client Sekretär</td></tr> <tr> <td>benötigt</td> <td>C1<>S1</td> <td>Client Betrieb<>Server Betrieb</td></tr> <tr> <td>benötigt</td> <td>C4<>D1</td> <td>Client Sekretär<>Drucker Betrieb</td></tr> <tr> <td>benötigt</td> <td>HP1<>C1/4/5</td> <td>Switch Betrieb<>Client Betrieb</td></tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td></tr> <tr> <td>Anwender</td> <td>Sekretär</td> <td>Peter Müller</td></tr> <tr> <td>Verantwortlicher</td> <td>Sekretär</td> <td>Peter Müller</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A04	TeamViewer	nötig für	A05	Word	benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb	benötigt	C1/4/5<>N1	Client Betrieb<>Firewall Betrieb	benötigt	C1<>C4	Client Betrieb<>Client Sekretär	benötigt	C1<>S1	Client Betrieb<>Server Betrieb	benötigt	C4<>D1	Client Sekretär<>Drucker Betrieb	benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb	Administrator	Admin	Sebastian Breu	Anwender	Sekretär	Peter Müller	Verantwortlicher	Sekretär	Peter Müller
Zuordnung	Kürzel	Name																																												
nötig für	GP03	Auftragsannahme / Verkauf																																												
nötig für	A01	Excel																																												
nötig für	A02	Outlook																																												
nötig für	A04	TeamViewer																																												
nötig für	A05	Word																																												
benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb																																												
benötigt	C1/4/5<>N1	Client Betrieb<>Firewall Betrieb																																												
benötigt	C1<>C4	Client Betrieb<>Client Sekretär																																												
benötigt	C1<>S1	Client Betrieb<>Server Betrieb																																												
benötigt	C4<>D1	Client Sekretär<>Drucker Betrieb																																												
benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb																																												
Administrator	Admin	Sebastian Breu																																												
Anwender	Sekretär	Peter Müller																																												
Verantwortlicher	Sekretär	Peter Müller																																												
C5	Client Geschäftsführung																																													
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td></tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td></tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td></tr> <tr> <td>nötig für</td> <td>A05</td> <td>Word</td></tr> <tr> <td>VM-Host für</td> <td>C5</td> <td>Client Geschäftsführung</td></tr> <tr> <td>benötigt</td> <td>C1/4/5<>AP2</td> <td>Client Betrieb<>WLAN AP Betrieb</td></tr> <tr> <td>benötigt</td> <td>C1/4/5<>N1</td> <td>Client Betrieb<>Firewall Betrieb</td></tr> <tr> <td>benötigt</td> <td>C1<>C5</td> <td>Client Betrieb<>Client Geschäftsführung</td></tr> <tr> <td>benötigt</td> <td>C1<>S1</td> <td>Client Betrieb<>Server Betrieb</td></tr> <tr> <td>benötigt</td> <td>C4<>C5</td> <td>Client Sekretär<>Client Geschäftsführung</td></tr> <tr> <td>benötigt</td> <td>C5<>D1</td> <td>Client Geschäftsführung<>Drucker Betrieb</td></tr> <tr> <td>benötigt</td> <td>HP1<>C1/4/5</td> <td>Switch Betrieb<>Client Betrieb</td></tr> <tr> <td>befindet sich in</td> <td>EG-1</td> <td>Büroraum Geschäftsleiter</td></tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A04	TeamViewer	nötig für	A05	Word	VM-Host für	C5	Client Geschäftsführung	benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb	benötigt	C1/4/5<>N1	Client Betrieb<>Firewall Betrieb	benötigt	C1<>C5	Client Betrieb<>Client Geschäftsführung	benötigt	C1<>S1	Client Betrieb<>Server Betrieb	benötigt	C4<>C5	Client Sekretär<>Client Geschäftsführung	benötigt	C5<>D1	Client Geschäftsführung<>Drucker Betrieb	benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb	befindet sich in	EG-1	Büroraum Geschäftsleiter	Administrator	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																																												
nötig für	A01	Excel																																												
nötig für	A02	Outlook																																												
nötig für	A04	TeamViewer																																												
nötig für	A05	Word																																												
VM-Host für	C5	Client Geschäftsführung																																												
benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb																																												
benötigt	C1/4/5<>N1	Client Betrieb<>Firewall Betrieb																																												
benötigt	C1<>C5	Client Betrieb<>Client Geschäftsführung																																												
benötigt	C1<>S1	Client Betrieb<>Server Betrieb																																												
benötigt	C4<>C5	Client Sekretär<>Client Geschäftsführung																																												
benötigt	C5<>D1	Client Geschäftsführung<>Drucker Betrieb																																												
benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb																																												
befindet sich in	EG-1	Büroraum Geschäftsleiter																																												
Administrator	Admin	Sebastian Breu																																												

Kürzel	Name																																							
C5	Client Geschäftsführung																																							
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>Anwender</td> <td>CEO</td> <td>Ulrich Meissen</td></tr> <tr> <td>Verantwortlicher</td> <td>CEO</td> <td>Ulrich Meissen</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	Anwender	CEO	Ulrich Meissen	Verantwortlicher	CEO	Ulrich Meissen																														
Zuordnung	Kürzel	Name																																						
Anwender	CEO	Ulrich Meissen																																						
Verantwortlicher	CEO	Ulrich Meissen																																						
C6	Client CNC Fräse																																							
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td></tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td></tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td></tr> <tr> <td>nötig für</td> <td>A03</td> <td>Delftship</td></tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td></tr> <tr> <td>benötigt</td> <td>S101</td> <td>Produktionsmaschine - CNC Fräse</td></tr> <tr> <td>benötigt</td> <td>C2/3/6/7<>AP1</td> <td>Client Produktion<>WLAN AP Produktion</td></tr> <tr> <td>benötigt</td> <td>C2<>C6</td> <td>Client Produktion<>Client CNC Fräse</td></tr> <tr> <td>benötigt</td> <td>C2<>C7</td> <td>Client Produktion<>Client Gussmaschine</td></tr> <tr> <td>benötigt</td> <td>C2<>S2</td> <td>Client Produktion<>Server Produktion</td></tr> <tr> <td>Verantwortlicher</td> <td></td> <td>Sylvia Gradl</td></tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP04	Fertigung	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A03	Delftship	nötig für	A04	TeamViewer	benötigt	S101	Produktionsmaschine - CNC Fräse	benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion	benötigt	C2<>C6	Client Produktion<>Client CNC Fräse	benötigt	C2<>C7	Client Produktion<>Client Gussmaschine	benötigt	C2<>S2	Client Produktion<>Server Produktion	Verantwortlicher		Sylvia Gradl	Administrator	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																																						
nötig für	GP04	Fertigung																																						
nötig für	A01	Excel																																						
nötig für	A02	Outlook																																						
nötig für	A03	Delftship																																						
nötig für	A04	TeamViewer																																						
benötigt	S101	Produktionsmaschine - CNC Fräse																																						
benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion																																						
benötigt	C2<>C6	Client Produktion<>Client CNC Fräse																																						
benötigt	C2<>C7	Client Produktion<>Client Gussmaschine																																						
benötigt	C2<>S2	Client Produktion<>Server Produktion																																						
Verantwortlicher		Sylvia Gradl																																						
Administrator	Admin	Sebastian Breu																																						
C7	Client Gussmaschine																																							
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td></tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td></tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td></tr> <tr> <td>nötig für</td> <td>A03</td> <td>Delftship</td></tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td></tr> <tr> <td>benötigt</td> <td>S102</td> <td>Produktionsmaschine - Gussmaschine</td></tr> <tr> <td>benötigt</td> <td>C2/3/6/7<>AP1</td> <td>Client Produktion<>WLAN AP Produktion</td></tr> <tr> <td>benötigt</td> <td>C2<>S2</td> <td>Client Produktion<>Server Produktion</td></tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP04	Fertigung	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A03	Delftship	nötig für	A04	TeamViewer	benötigt	S102	Produktionsmaschine - Gussmaschine	benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion	benötigt	C2<>S2	Client Produktion<>Server Produktion	Administrator	Admin	Sebastian Breu									
Zuordnung	Kürzel	Name																																						
nötig für	GP04	Fertigung																																						
nötig für	A01	Excel																																						
nötig für	A02	Outlook																																						
nötig für	A03	Delftship																																						
nötig für	A04	TeamViewer																																						
benötigt	S102	Produktionsmaschine - Gussmaschine																																						
benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion																																						
benötigt	C2<>S2	Client Produktion<>Server Produktion																																						
Administrator	Admin	Sebastian Breu																																						
D1	Drucker Betrieb																																							
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP02</td> <td>Einkauf</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP02	Einkauf																																	
Zuordnung	Kürzel	Name																																						
nötig für	GP02	Einkauf																																						

Kürzel	Name																														
D1	Drucker Betrieb																														
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td></tr> <tr> <td>benötigt</td> <td>N1</td> <td>Firewall Betrieb</td></tr> <tr> <td>nötig für</td> <td>S1</td> <td>Server Betrieb</td></tr> <tr> <td>benötigt</td> <td>C1<>D1</td> <td>Client Betrieb<>Drucker Betrieb</td></tr> <tr> <td>benötigt</td> <td>C4<>D1</td> <td>Client Sekräter<>Drucker Betrieb</td></tr> <tr> <td>benötigt</td> <td>C5<>D1</td> <td>Client Geschäftsführung<>Drucker Betrieb</td></tr> <tr> <td>Anwender</td> <td></td> <td>Ulrike Schmidt</td></tr> <tr> <td>Verantwortlicher</td> <td>Admin</td> <td>Sebastian Breu</td></tr> <tr> <td>Anwender</td> <td>HR</td> <td>Michael Holzhüter</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP03	Auftragsannahme / Verkauf	benötigt	N1	Firewall Betrieb	nötig für	S1	Server Betrieb	benötigt	C1<>D1	Client Betrieb<>Drucker Betrieb	benötigt	C4<>D1	Client Sekräter<>Drucker Betrieb	benötigt	C5<>D1	Client Geschäftsführung<>Drucker Betrieb	Anwender		Ulrike Schmidt	Verantwortlicher	Admin	Sebastian Breu	Anwender	HR	Michael Holzhüter
Zuordnung	Kürzel	Name																													
nötig für	GP03	Auftragsannahme / Verkauf																													
benötigt	N1	Firewall Betrieb																													
nötig für	S1	Server Betrieb																													
benötigt	C1<>D1	Client Betrieb<>Drucker Betrieb																													
benötigt	C4<>D1	Client Sekräter<>Drucker Betrieb																													
benötigt	C5<>D1	Client Geschäftsführung<>Drucker Betrieb																													
Anwender		Ulrike Schmidt																													
Verantwortlicher	Admin	Sebastian Breu																													
Anwender	HR	Michael Holzhüter																													
D2	Drucker Produktion																														
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>C2</td> <td>Client Produktion</td></tr> <tr> <td>benötigt</td> <td>N2</td> <td>Firewall Produktion</td></tr> <tr> <td>benötigt</td> <td>S2</td> <td>Server Produktion</td></tr> <tr> <td>benötigt</td> <td>C2<>D2</td> <td>Client Produktion<>Drucker Produktion</td></tr> <tr> <td>benötigt</td> <td>C3<>D2</td> <td>Client Produktionsleiter<>Drucker Produktion</td></tr> <tr> <td>Anwender</td> <td></td> <td>Nicolas Traidl</td></tr> <tr> <td>Verantwortlicher</td> <td>Admin</td> <td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	C2	Client Produktion	benötigt	N2	Firewall Produktion	benötigt	S2	Server Produktion	benötigt	C2<>D2	Client Produktion<>Drucker Produktion	benötigt	C3<>D2	Client Produktionsleiter<>Drucker Produktion	Anwender		Nicolas Traidl	Verantwortlicher	Admin	Sebastian Breu						
Zuordnung	Kürzel	Name																													
nötig für	C2	Client Produktion																													
benötigt	N2	Firewall Produktion																													
benötigt	S2	Server Produktion																													
benötigt	C2<>D2	Client Produktion<>Drucker Produktion																													
benötigt	C3<>D2	Client Produktionsleiter<>Drucker Produktion																													
Anwender		Nicolas Traidl																													
Verantwortlicher	Admin	Sebastian Breu																													
HP1	Switch Betrieb																														
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>AP2</td> <td>WLAN Access Point Betrieb</td></tr> <tr> <td>benötigt</td> <td>N1</td> <td>Firewall Betrieb</td></tr> <tr> <td>nötig für</td> <td>S1</td> <td>Server Betrieb</td></tr> <tr> <td>benötigt</td> <td>HP1<>C1/4/5</td> <td>Switch Betrieb<>Client Betrieb</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	AP2	WLAN Access Point Betrieb	benötigt	N1	Firewall Betrieb	nötig für	S1	Server Betrieb	benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb															
Zuordnung	Kürzel	Name																													
nötig für	AP2	WLAN Access Point Betrieb																													
benötigt	N1	Firewall Betrieb																													
nötig für	S1	Server Betrieb																													
benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb																													
HP2	Switch Produktion																														
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>AP1</td> <td>WLAN Access Point Produktion</td></tr> <tr> <td>benötigt</td> <td>N2</td> <td>Firewall Produktion</td></tr> <tr> <td>nötig für</td> <td>S2</td> <td>Server Produktion</td></tr> <tr> <td>benötigt</td> <td>HP2<>C2/3</td> <td>Switch Produktion<>Client Produktion</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	AP1	WLAN Access Point Produktion	benötigt	N2	Firewall Produktion	nötig für	S2	Server Produktion	benötigt	HP2<>C2/3	Switch Produktion<>Client Produktion															
Zuordnung	Kürzel	Name																													
nötig für	AP1	WLAN Access Point Produktion																													
benötigt	N2	Firewall Produktion																													
nötig für	S2	Server Produktion																													
benötigt	HP2<>C2/3	Switch Produktion<>Client Produktion																													

Kürzel	Name
N1	Firewall Betrieb
Zuordnung	Kürzel
nötig für	GP02
nötig für	GP03
nötig für	GP05
nötig für	AP2
nötig für	D1
nötig für	HP1
benötigt	R1
nötig für	S1
benötigt	C1/4/5<>N1
benötigt	K43
benötigt	K45
benötigt	K46
benötigt	S1<>N1
befindet sich in	OG-5
Administrator	Admin
N2	Firewall Produktion
Zuordnung	Kürzel
nötig für	GP01
nötig für	GP04
nötig für	AP1
nötig für	D2
nötig für	HP2
benötigt	R1
virtualisiert auf	S2
benötigt	C2/C3/C6/C7<>N2
benötigt	K40
benötigt	K43
benötigt	K46
benötigt	S2<>N2
befindet sich in	OG-5

Kürzel	Name																																										
N2	Firewall Produktion																																										
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	Administrator	Admin	Sebastian Breu																																				
Zuordnung	Kürzel	Name																																									
Administrator	Admin	Sebastian Breu																																									
R1	Router																																										
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP01</td> <td>Konstruktion</td> </tr> <tr> <td>nötig für</td> <td>GP02</td> <td>Einkauf</td> </tr> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td> </tr> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td> </tr> <tr> <td>nötig für</td> <td>GP05</td> <td>Technischer Support</td> </tr> <tr> <td>nötig für</td> <td>N1</td> <td>Firewall Betrieb</td> </tr> <tr> <td>nötig für</td> <td>N2</td> <td>Firewall Produktion</td> </tr> <tr> <td>benötigt</td> <td>K40</td> <td>Firewall Prod <> Router</td> </tr> <tr> <td>benötigt</td> <td>K42</td> <td>Router<>Videoüberwachung</td> </tr> <tr> <td>benötigt</td> <td>K43</td> <td>Router<>Internet</td> </tr> <tr> <td>benötigt</td> <td>K45</td> <td>Firewall Betrieb<->Router</td> </tr> <tr> <td>befindet sich in</td> <td>OG-5</td> <td>Serverraum</td> </tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP01	Konstruktion	nötig für	GP02	Einkauf	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	GP04	Fertigung	nötig für	GP05	Technischer Support	nötig für	N1	Firewall Betrieb	nötig für	N2	Firewall Produktion	benötigt	K40	Firewall Prod <> Router	benötigt	K42	Router<>Videoüberwachung	benötigt	K43	Router<>Internet	benötigt	K45	Firewall Betrieb<->Router	befindet sich in	OG-5	Serverraum	Administrator	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																																									
nötig für	GP01	Konstruktion																																									
nötig für	GP02	Einkauf																																									
nötig für	GP03	Auftragsannahme / Verkauf																																									
nötig für	GP04	Fertigung																																									
nötig für	GP05	Technischer Support																																									
nötig für	N1	Firewall Betrieb																																									
nötig für	N2	Firewall Produktion																																									
benötigt	K40	Firewall Prod <> Router																																									
benötigt	K42	Router<>Videoüberwachung																																									
benötigt	K43	Router<>Internet																																									
benötigt	K45	Firewall Betrieb<->Router																																									
befindet sich in	OG-5	Serverraum																																									
Administrator	Admin	Sebastian Breu																																									
S1	Server Betrieb																																										
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP02</td> <td>Einkauf</td> </tr> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td> </tr> <tr> <td>nötig für</td> <td>GP05</td> <td>Technischer Support</td> </tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td> </tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td> </tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td> </tr> <tr> <td>nötig für</td> <td>A05</td> <td>Word</td> </tr> <tr> <td>benötigt</td> <td>D1</td> <td>Drucker Betrieb</td> </tr> <tr> <td>benötigt</td> <td>HP1</td> <td>Switch Betrieb</td> </tr> <tr> <td>benötigt</td> <td>N1</td> <td>Firewall Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C1<>S1</td> <td>Client Betrieb<>Server Betrieb</td> </tr> <tr> <td>benötigt</td> <td>S1<>N1</td> <td>Server Betrieb<>Firewall Betrieb</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP02	Einkauf	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	GP05	Technischer Support	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A04	TeamViewer	nötig für	A05	Word	benötigt	D1	Drucker Betrieb	benötigt	HP1	Switch Betrieb	benötigt	N1	Firewall Betrieb	benötigt	C1<>S1	Client Betrieb<>Server Betrieb	benötigt	S1<>N1	Server Betrieb<>Firewall Betrieb			
Zuordnung	Kürzel	Name																																									
nötig für	GP02	Einkauf																																									
nötig für	GP03	Auftragsannahme / Verkauf																																									
nötig für	GP05	Technischer Support																																									
nötig für	A01	Excel																																									
nötig für	A02	Outlook																																									
nötig für	A04	TeamViewer																																									
nötig für	A05	Word																																									
benötigt	D1	Drucker Betrieb																																									
benötigt	HP1	Switch Betrieb																																									
benötigt	N1	Firewall Betrieb																																									
benötigt	C1<>S1	Client Betrieb<>Server Betrieb																																									
benötigt	S1<>N1	Server Betrieb<>Firewall Betrieb																																									

Kürzel	Name																																													
S1	Server Betrieb																																													
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>benötigt</td> <td>S1<>S2</td> <td>Server Betrieb<>Server Produktion</td></tr> <tr> <td>befindet sich in</td> <td>OG-5</td> <td>Serverraum</td></tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	benötigt	S1<>S2	Server Betrieb<>Server Produktion	befindet sich in	OG-5	Serverraum	Administrator	Admin	Sebastian Breu																																	
Zuordnung	Kürzel	Name																																												
benötigt	S1<>S2	Server Betrieb<>Server Produktion																																												
befindet sich in	OG-5	Serverraum																																												
Administrator	Admin	Sebastian Breu																																												
S2	Server Produktion																																													
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP01</td> <td>Konstruktion</td></tr> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td></tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td></tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td></tr> <tr> <td>nötig für</td> <td>A03</td> <td>Delftship</td></tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td></tr> <tr> <td>nötig für</td> <td>D2</td> <td>Drucker Produktion</td></tr> <tr> <td>benötigt</td> <td>HP2</td> <td>Switch Produktion</td></tr> <tr> <td>VM-Host für</td> <td>N2</td> <td>Firewall Produktion</td></tr> <tr> <td>benötigt</td> <td>C2<>S2</td> <td>Client Produktion<>Server Produktion</td></tr> <tr> <td>benötigt</td> <td>S1<>S2</td> <td>Server Betrieb<>Server Produktion</td></tr> <tr> <td>benötigt</td> <td>S2<=>N2</td> <td>Server Produktion<>Firewall Produktion</td></tr> <tr> <td>befindet sich in</td> <td></td> <td>Halle und Materiallager</td></tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP01	Konstruktion	nötig für	GP04	Fertigung	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A03	Delftship	nötig für	A04	TeamViewer	nötig für	D2	Drucker Produktion	benötigt	HP2	Switch Produktion	VM-Host für	N2	Firewall Produktion	benötigt	C2<>S2	Client Produktion<>Server Produktion	benötigt	S1<>S2	Server Betrieb<>Server Produktion	benötigt	S2<=>N2	Server Produktion<>Firewall Produktion	befindet sich in		Halle und Materiallager	Administrator	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																																												
nötig für	GP01	Konstruktion																																												
nötig für	GP04	Fertigung																																												
nötig für	A01	Excel																																												
nötig für	A02	Outlook																																												
nötig für	A03	Delftship																																												
nötig für	A04	TeamViewer																																												
nötig für	D2	Drucker Produktion																																												
benötigt	HP2	Switch Produktion																																												
VM-Host für	N2	Firewall Produktion																																												
benötigt	C2<>S2	Client Produktion<>Server Produktion																																												
benötigt	S1<>S2	Server Betrieb<>Server Produktion																																												
benötigt	S2<=>N2	Server Produktion<>Firewall Produktion																																												
befindet sich in		Halle und Materiallager																																												
Administrator	Admin	Sebastian Breu																																												

ICS-System

Kürzel	Name																		
S101	Produktionsmaschine - CNC Fräse																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td></tr> <tr> <td>nötig für</td> <td>C6</td> <td>Client CNC Fräse</td></tr> <tr> <td>benötigt</td> <td>C2/3<=>S100/S101/102</td> <td>Client Produktion/Produktionsleiter<>ICS-Systeme</td></tr> <tr> <td>befindet sich in</td> <td></td> <td>Halle und Materiallager</td></tr> <tr> <td>Verantwortlicher</td> <td></td> <td>Sylvia Gradl</td></tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP04	Fertigung	nötig für	C6	Client CNC Fräse	benötigt	C2/3<=>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme	befindet sich in		Halle und Materiallager	Verantwortlicher		Sylvia Gradl
Zuordnung	Kürzel	Name																	
nötig für	GP04	Fertigung																	
nötig für	C6	Client CNC Fräse																	
benötigt	C2/3<=>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme																	
befindet sich in		Halle und Materiallager																	
Verantwortlicher		Sylvia Gradl																	

Kürzel	Name																		
S102	Produktionsmaschine - Gussmaschine																		
	<table> <tr> <td>Zuordnung</td> <td>Kürzel</td> <td>Name</td> </tr> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td> </tr> <tr> <td>nötig für</td> <td>C7</td> <td>Client Gussmaschine</td> </tr> <tr> <td>benötigt</td> <td>C2/3<>S100/S101/102</td> <td>Client Produktion/Produktionsleiter<>ICS-Systeme</td> </tr> <tr> <td>befindet sich in</td> <td></td> <td>Halle und Materiallager</td> </tr> <tr> <td>Verantwortlicher</td> <td></td> <td>Sylvia Gradl</td> </tr> </table>	Zuordnung	Kürzel	Name	nötig für	GP04	Fertigung	nötig für	C7	Client Gussmaschine	benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme	befindet sich in		Halle und Materiallager	Verantwortlicher		Sylvia Gradl
Zuordnung	Kürzel	Name																	
nötig für	GP04	Fertigung																	
nötig für	C7	Client Gussmaschine																	
benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme																	
befindet sich in		Halle und Materiallager																	
Verantwortlicher		Sylvia Gradl																	
S100	SPS																		
	<table> <tr> <td>Zuordnung</td> <td>Kürzel</td> <td>Name</td> </tr> <tr> <td>nötig für</td> <td>GP04</td> <td>Fertigung</td> </tr> <tr> <td>benötigt</td> <td>C2/3<>S100/S101/102</td> <td>Client Produktion/Produktionsleiter<>ICS-Systeme</td> </tr> <tr> <td>befindet sich in</td> <td></td> <td>Halle und Materiallager</td> </tr> <tr> <td>Verantwortlicher</td> <td></td> <td>Sylvia Gradl</td> </tr> </table>	Zuordnung	Kürzel	Name	nötig für	GP04	Fertigung	benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme	befindet sich in		Halle und Materiallager	Verantwortlicher		Sylvia Gradl			
Zuordnung	Kürzel	Name																	
nötig für	GP04	Fertigung																	
benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme																	
befindet sich in		Halle und Materiallager																	
Verantwortlicher		Sylvia Gradl																	

Anderes/IoT-System

Kürzel	Name									
I1	Videoüberwachung									
	<table> <tr> <td>Zuordnung</td> <td>Kürzel</td> <td>Name</td> </tr> <tr> <td>benötigt</td> <td>K42</td> <td>Router<>Videoüberwachung</td> </tr> </table>	Zuordnung	Kürzel	Name	benötigt	K42	Router<>Videoüberwachung			
Zuordnung	Kürzel	Name								
benötigt	K42	Router<>Videoüberwachung								
K1	Kaffeemaschine									
	<table> <tr> <td>Zuordnung</td> <td>Kürzel</td> <td>Name</td> </tr> <tr> <td>benötigt</td> <td>K44</td> <td>Kaffeemaschine <> WLAN AP PROD</td> </tr> <tr> <td>befindet sich in</td> <td>EG-6</td> <td>Küche</td> </tr> </table>	Zuordnung	Kürzel	Name	benötigt	K44	Kaffeemaschine <> WLAN AP PROD	befindet sich in	EG-6	Küche
Zuordnung	Kürzel	Name								
benötigt	K44	Kaffeemaschine <> WLAN AP PROD								
befindet sich in	EG-6	Küche								

Kommunikationsverbindungen

Kürzel	Name			
AP1<>N1	WLAN AP Betrieb<>Firewall Betrieb			
	<table> <tr> <td>Zuordnung</td> <td>Kürzel</td> <td>Name</td> </tr> </table>	Zuordnung	Kürzel	Name
Zuordnung	Kürzel	Name		
AP2<>N2	WLAN AP Produktion<>Firewall Produktion			
	<table> <tr> <td>Zuordnung</td> <td>Kürzel</td> <td>Name</td> </tr> </table>	Zuordnung	Kürzel	Name
Zuordnung	Kürzel	Name		

Kürzel	Name	
C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb	
Zuordnung	Kürzel	Name
nötig für	AP2	WLAN Access Point Betrieb
nötig für	C1	Client Betrieb APC
nötig für	C1	Client Betrieb Laptop
nötig für	C4	Client Sekretär
nötig für	C5	Client Geschäftsführung
C1/4/5<>N1	Client Betrieb<>Firewall Betrieb	
Zuordnung	Kürzel	Name
nötig für	GP02	Einkauf
nötig für	GP03	Auftragsannahme / Verkauf
nötig für	GP05	Technischer Support
nötig für	C1	Client Betrieb APC
nötig für	C1	Client Betrieb Laptop
nötig für	C4	Client Sekretär
nötig für	C5	Client Geschäftsführung
nötig für	N1	Firewall Betrieb
C1<>C2	Client Betrieb<>Client Produktion	
Zuordnung	Kürzel	Name
nötig für	C1	Client Betrieb APC
nötig für	C1	Client Betrieb Laptop
nötig für	C2	Client Produktion
C1<>C4	Client Betrieb<>Client Sekretär	
Zuordnung	Kürzel	Name
nötig für	C1	Client Betrieb APC
nötig für	C1	Client Betrieb Laptop
nötig für	C4	Client Sekretär
C1<>C5	Client Betrieb<>Client Geschäftsführung	
Zuordnung	Kürzel	Name
nötig für	C1	Client Betrieb APC
nötig für	C1	Client Betrieb Laptop
nötig für	C5	Client Geschäftsführung

Kürzel	Name																		
C1<>D1	Client Betrieb<>Drucker Betrieb																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>C1</td> <td>Client Betrieb APC</td> </tr> <tr> <td>nötig für</td> <td>C1</td> <td>Client Betrieb Laptop</td> </tr> <tr> <td>nötig für</td> <td>D1</td> <td>Drucker Betrieb</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	C1	Client Betrieb APC	nötig für	C1	Client Betrieb Laptop	nötig für	D1	Drucker Betrieb						
Zuordnung	Kürzel	Name																	
nötig für	C1	Client Betrieb APC																	
nötig für	C1	Client Betrieb Laptop																	
nötig für	D1	Drucker Betrieb																	
C1<>S1	Client Betrieb<>Server Betrieb																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>C1</td> <td>Client Betrieb APC</td> </tr> <tr> <td>nötig für</td> <td>C1</td> <td>Client Betrieb Laptop</td> </tr> <tr> <td>nötig für</td> <td>C4</td> <td>Client Sekretär</td> </tr> <tr> <td>nötig für</td> <td>C5</td> <td>Client Geschäftsführung</td> </tr> <tr> <td>nötig für</td> <td>S1</td> <td>Server Betrieb</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	C1	Client Betrieb APC	nötig für	C1	Client Betrieb Laptop	nötig für	C4	Client Sekretär	nötig für	C5	Client Geschäftsführung	nötig für	S1	Server Betrieb
Zuordnung	Kürzel	Name																	
nötig für	C1	Client Betrieb APC																	
nötig für	C1	Client Betrieb Laptop																	
nötig für	C4	Client Sekretär																	
nötig für	C5	Client Geschäftsführung																	
nötig für	S1	Server Betrieb																	
C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>AP1</td> <td>WLAN Access Point Produktion</td> </tr> <tr> <td>nötig für</td> <td>C2</td> <td>Client Produktion</td> </tr> <tr> <td>nötig für</td> <td>C3</td> <td>Client Produktionsleiter</td> </tr> <tr> <td>nötig für</td> <td>C6</td> <td>Client CNC Fräse</td> </tr> <tr> <td>nötig für</td> <td>C7</td> <td>Client Gussmaschine</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	AP1	WLAN Access Point Produktion	nötig für	C2	Client Produktion	nötig für	C3	Client Produktionsleiter	nötig für	C6	Client CNC Fräse	nötig für	C7	Client Gussmaschine
Zuordnung	Kürzel	Name																	
nötig für	AP1	WLAN Access Point Produktion																	
nötig für	C2	Client Produktion																	
nötig für	C3	Client Produktionsleiter																	
nötig für	C6	Client CNC Fräse																	
nötig für	C7	Client Gussmaschine																	
C2/3<>S100/ S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>C2</td> <td>Client Produktion</td> </tr> <tr> <td>nötig für</td> <td>C3</td> <td>Client Produktionsleiter</td> </tr> <tr> <td>nötig für</td> <td>S100</td> <td>SPS</td> </tr> <tr> <td>nötig für</td> <td>S101</td> <td>Produktionsmaschine - CNC Fräse</td> </tr> <tr> <td>nötig für</td> <td>S102</td> <td>Produktionsmaschine - Gussmaschine</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	C2	Client Produktion	nötig für	C3	Client Produktionsleiter	nötig für	S100	SPS	nötig für	S101	Produktionsmaschine - CNC Fräse	nötig für	S102	Produktionsmaschine - Gussmaschine
Zuordnung	Kürzel	Name																	
nötig für	C2	Client Produktion																	
nötig für	C3	Client Produktionsleiter																	
nötig für	S100	SPS																	
nötig für	S101	Produktionsmaschine - CNC Fräse																	
nötig für	S102	Produktionsmaschine - Gussmaschine																	
C2/C3/C6/ C7<>N2	Client Produktion<>Firewall Produktion																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>C2</td> <td>Client Produktion</td> </tr> <tr> <td>nötig für</td> <td>C3</td> <td>Client Produktionsleiter</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	C2	Client Produktion	nötig für	C3	Client Produktionsleiter									
Zuordnung	Kürzel	Name																	
nötig für	C2	Client Produktion																	
nötig für	C3	Client Produktionsleiter																	

Kürzel	Name	
C2/C3/C6/ C7<>N2	Client Produktion<>Firewall Produktion	
Zuordnung nötig für	Kürzel N2	Name Firewall Produktion
C2<>C3	Client Produktion<>Client Produktionsleiter	
Zuordnung nötig für nötig für	Kürzel C2 C3	Name Client Produktion Client Produktionsleiter
C2<>C6	Client Produktion<>Client CNC Fräse	
Zuordnung nötig für nötig für	Kürzel C2 C6	Name Client Produktion Client CNC Fräse
C2<>C7	Client Produktion<>Client Gussmaschine	
Zuordnung nötig für nötig für	Kürzel C2 C6	Name Client Produktion Client CNC Fräse
C2<>D2	Client Produktion<>Drucker Produktion	
Zuordnung nötig für nötig für	Kürzel C2 D2	Name Client Produktion Drucker Produktion
C2<>S2	Client Produktion<>Server Produktion	
Zuordnung nötig für nötig für nötig für nötig für nötig für	Kürzel C2 C3 C6 C7 S2	Name Client Produktion Client Produktionsleiter Client CNC Fräse Client Gussmaschine Server Produktion
C3<>D2	Client Produktionsleiter<>Drucker Produktion	
Zuordnung nötig für nötig für	Kürzel C3 D2	Name Client Produktionsleiter Drucker Produktion

Kürzel	Name																		
C4<>C5	Client Sekretär<>Client Geschäftsführung																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>C1</td> <td>Client Betrieb APC</td> </tr> <tr> <td>nötig für</td> <td>C1</td> <td>Client Betrieb Laptop</td> </tr> <tr> <td>nötig für</td> <td>C5</td> <td>Client Geschäftsführung</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	C1	Client Betrieb APC	nötig für	C1	Client Betrieb Laptop	nötig für	C5	Client Geschäftsführung						
Zuordnung	Kürzel	Name																	
nötig für	C1	Client Betrieb APC																	
nötig für	C1	Client Betrieb Laptop																	
nötig für	C5	Client Geschäftsführung																	
C4<>D1	Client Sekräter<>Drucker Betrieb																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>C4</td> <td>Client Sekretär</td> </tr> <tr> <td>nötig für</td> <td>D1</td> <td>Drucker Betrieb</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	C4	Client Sekretär	nötig für	D1	Drucker Betrieb									
Zuordnung	Kürzel	Name																	
nötig für	C4	Client Sekretär																	
nötig für	D1	Drucker Betrieb																	
C5<>D1	Client Geschäftsführung<>Drucker Betrieb																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>C5</td> <td>Client Geschäftsführung</td> </tr> <tr> <td>nötig für</td> <td>D1</td> <td>Drucker Betrieb</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	C5	Client Geschäftsführung	nötig für	D1	Drucker Betrieb									
Zuordnung	Kürzel	Name																	
nötig für	C5	Client Geschäftsführung																	
nötig für	D1	Drucker Betrieb																	
HP1<>AP2	Switch Betrieb<>WLAN AP Betrieb																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>befindet sich in</td> <td>OG-5</td> <td>Serverraum</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	befindet sich in	OG-5	Serverraum												
Zuordnung	Kürzel	Name																	
befindet sich in	OG-5	Serverraum																	
HP1<>C1/4/5	Switch Betrieb<>Client Betrieb																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>C1</td> <td>Client Betrieb APC</td> </tr> <tr> <td>nötig für</td> <td>C1</td> <td>Client Betrieb Laptop</td> </tr> <tr> <td>nötig für</td> <td>C4</td> <td>Client Sekretär</td> </tr> <tr> <td>nötig für</td> <td>C5</td> <td>Client Geschäftsführung</td> </tr> <tr> <td>nötig für</td> <td>HP1</td> <td>Switch Betrieb</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	C1	Client Betrieb APC	nötig für	C1	Client Betrieb Laptop	nötig für	C4	Client Sekretär	nötig für	C5	Client Geschäftsführung	nötig für	HP1	Switch Betrieb
Zuordnung	Kürzel	Name																	
nötig für	C1	Client Betrieb APC																	
nötig für	C1	Client Betrieb Laptop																	
nötig für	C4	Client Sekretär																	
nötig für	C5	Client Geschäftsführung																	
nötig für	HP1	Switch Betrieb																	
HP1<>D1	Switch Betrieb<>Drucker Betrieb																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> </table>	Zuordnung	Kürzel	Name															
Zuordnung	Kürzel	Name																	
HP1<>N1	Server Betrieb<>Firewall Betrieb																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> </table>	Zuordnung	Kürzel	Name															
Zuordnung	Kürzel	Name																	
HP1<>S1	Switch Betrieb<>Server Betrieb																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> </table>	Zuordnung	Kürzel	Name															
Zuordnung	Kürzel	Name																	
HP2<->AP1	Switch Produktion<>WLAN AP Produktion																		
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> </table>	Zuordnung	Kürzel	Name															
Zuordnung	Kürzel	Name																	

Kürzel	Name
HP2<>C2/3	Switch Produktion<>Client Produktion
Zuordnung	Kürzel
nötig für	C2
nötig für	C3
nötig für	HP2
	Name
	Client Produktion
	Client Produktionsleiter
	Switch Produktion
HP2<>N2	Switch Betrieb<>Firewall Betrieb
Zuordnung	Kürzel
	Name
HP2<>S2	Switch Produktion<>Drucker Produktion
Zuordnung	Kürzel
	Name
HP2<>S2	Switch Produktion<>Server Produktion
Zuordnung	Kürzel
	Name
K40	Firewall Prod <> Router
Zuordnung	Kürzel
nötig für	GP01
nötig für	GP04
nötig für	N2
nötig für	R1
	Name
	Konstruktion
	Fertigung
	Firewall Produktion
	Router
K42	Router<>Videoüberwachung
Zuordnung	Kürzel
	Name
nötig für	R1
nötig für	I1
	Router
	Videoüberwachung
K43	Router<>Internet
Zuordnung	Kürzel
nötig für	N1
nötig für	N2
nötig für	R1
	Name
	Firewall Betrieb
	Firewall Produktion
	Router
K44	Kaffeemaschine <> WLAN AP PROD
Zuordnung	Kürzel
nötig für	AP1
nötig für	K1
	Name
	WLAN Access Point Produktion
	Kaffeemaschine

Kürzel	Name
K45	Firewall Betrieb<->Router
Zuordnung	Kürzel
nötig für	GP02
nötig für	GP03
nötig für	GP05
nötig für	N1
nötig für	R1
	Name
	Einkauf
	Auftragsannahme / Verkauf
	Technischer Support
	Firewall Betrieb
	Router
K46	Firewall Betrieb<=>Firewall Produktion
Zuordnung	Kürzel
nötig für	N1
nötig für	N2
	Name
	Firewall Betrieb
	Firewall Produktion
S1<>N1	Server Betrieb<=>Firewall Betrieb
Zuordnung	Kürzel
nötig für	N1
nötig für	S1
	Name
	Firewall Betrieb
	Server Betrieb
S1<>S2	Server Betrieb<=>Server Produktion
Zuordnung	Kürzel
nötig für	S1
nötig für	S2
	Name
	Server Betrieb
	Server Produktion
S2<>N2	Server Produktion<=>Firewall Produktion
Zuordnung	Kürzel
nötig für	N2
nötig für	S2
	Name
	Firewall Produktion
	Server Produktion

Räume

Kürzel	Name
	Halle und Materiallager
Zuordnung	Kürzel
beinhaltet	S2
beinhaltet	S100
beinhaltet	S101
	Name
	Server Produktion
	SPS
	Produktionsmaschine - CNC Fräse

Kürzel	Name		
	Halle und Materiallager		
	Zuordnung beinhaltet	Kürzel S102	Name Produktionsmaschine - Gussmaschine
EG-1	Büro Raum Geschäftsführer		
	Zuordnung beinhaltet Hauptverantwortlicher	Kürzel C5 CEO	Name Client Geschäftsführung Ulrich Meissen
EG-2	Büro Raum Personal		
	Zuordnung Hauptverantwortlicher	Kürzel HR	Name Michael Holzhüter
EG-3	Büro Raum Entwicklung		
	Zuordnung Hauptverantwortlicher	Kürzel	Name Mia Lindenberg
EG-4	Büro Raum Einkauf		
	Zuordnung Hauptverantwortlicher	Kürzel	Name Lieselotte Hans
EG-5	Empfang/Wartebereich		
	Zuordnung Hauptverantwortlicher	Kürzel Sekretär	Name Peter Müller
EG-6	Küche		
	Zuordnung beinhaltet	Kürzel K1	Name Kaffeemaschine
LG-1	Büro Raum Produktion		
	Zuordnung Hauptverantwortlicher	Kürzel	Name Sylvia Gradl
LG-2	Küche		
	Zuordnung	Kürzel	Name
OG-1	Büro Raum Vertrieb		
	Zuordnung Hauptverantwortlicher	Kürzel	Name Heinrich Henckel von Donnersmarck

Kürzel	Name																					
OG-2	Büroraum IT Admin																					
	<table> <tr> <td>Zuordnung</td><td>Kürzel</td><td>Name</td></tr> <tr> <td>Hauptverantwortlicher</td><td>Admin</td><td>Sebastian Breu</td></tr> </table>	Zuordnung	Kürzel	Name	Hauptverantwortlicher	Admin	Sebastian Breu															
Zuordnung	Kürzel	Name																				
Hauptverantwortlicher	Admin	Sebastian Breu																				
OG-3	Büroraum CISO																					
	<table> <tr> <td>Zuordnung</td><td>Kürzel</td><td>Name</td></tr> <tr> <td>Hauptverantwortlicher</td><td>CISO</td><td>Gruppe 4</td></tr> </table>	Zuordnung	Kürzel	Name	Hauptverantwortlicher	CISO	Gruppe 4															
Zuordnung	Kürzel	Name																				
Hauptverantwortlicher	CISO	Gruppe 4																				
OG-4	Pausenraum																					
	<table> <tr> <td>Zuordnung</td><td>Kürzel</td><td>Name</td></tr> </table>	Zuordnung	Kürzel	Name																		
Zuordnung	Kürzel	Name																				
OG-5	Serverraum																					
	<table> <tr> <td>Zuordnung</td><td>Kürzel</td><td>Name</td></tr> <tr> <td>beinhaltet</td><td>N1</td><td>Firewall Betrieb</td></tr> <tr> <td>beinhaltet</td><td>N2</td><td>Firewall Produktion</td></tr> <tr> <td>beinhaltet</td><td>R1</td><td>Router</td></tr> <tr> <td>beinhaltet</td><td>S1</td><td>Server Betrieb</td></tr> <tr> <td>beinhaltet</td><td>HP1<math>\leftrightarrow</math>AP2</td><td>Switch Betrieb<math>\leftrightarrow</math>WLAN AP Betrieb</td></tr> <tr> <td>Hauptverantwortlicher</td><td>Admin</td><td>Sebastian Breu</td></tr> </table>	Zuordnung	Kürzel	Name	beinhaltet	N1	Firewall Betrieb	beinhaltet	N2	Firewall Produktion	beinhaltet	R1	Router	beinhaltet	S1	Server Betrieb	beinhaltet	HP1\leftrightarrowAP2	Switch Betrieb\leftrightarrowWLAN AP Betrieb	Hauptverantwortlicher	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																				
beinhaltet	N1	Firewall Betrieb																				
beinhaltet	N2	Firewall Produktion																				
beinhaltet	R1	Router																				
beinhaltet	S1	Server Betrieb																				
beinhaltet	HP1\leftrightarrowAP2	Switch Betrieb\leftrightarrowWLAN AP Betrieb																				
Hauptverantwortlicher	Admin	Sebastian Breu																				

Personen

Kürzel	Name									
	Ulrike Schmidt									
	<table> <tr> <td>Zuordnung</td><td>Kürzel</td><td>Name</td></tr> <tr> <td>Anwender von</td><td>C1</td><td>Client Betrieb Laptop</td></tr> <tr> <td>Anwender von</td><td>D1</td><td>Drucker Betrieb</td></tr> </table>	Zuordnung	Kürzel	Name	Anwender von	C1	Client Betrieb Laptop	Anwender von	D1	Drucker Betrieb
Zuordnung	Kürzel	Name								
Anwender von	C1	Client Betrieb Laptop								
Anwender von	D1	Drucker Betrieb								
	Monica Berns									
	<table> <tr> <td>Zuordnung</td><td>Kürzel</td><td>Name</td></tr> <tr> <td>Anwender von</td><td>C1</td><td>Client Betrieb Laptop</td></tr> <tr> <td>Anwender von</td><td>D1</td><td>Drucker Betrieb</td></tr> </table>	Zuordnung	Kürzel	Name	Anwender von	C1	Client Betrieb Laptop	Anwender von	D1	Drucker Betrieb
Zuordnung	Kürzel	Name								
Anwender von	C1	Client Betrieb Laptop								
Anwender von	D1	Drucker Betrieb								
	Sebastian Severing									
	<table> <tr> <td>Zuordnung</td><td>Kürzel</td><td>Name</td></tr> <tr> <td>Anwender von</td><td>C1</td><td>Client Betrieb Laptop</td></tr> <tr> <td>Anwender von</td><td>D1</td><td>Drucker Betrieb</td></tr> </table>	Zuordnung	Kürzel	Name	Anwender von	C1	Client Betrieb Laptop	Anwender von	D1	Drucker Betrieb
Zuordnung	Kürzel	Name								
Anwender von	C1	Client Betrieb Laptop								
Anwender von	D1	Drucker Betrieb								

Kürzel	Name	
Mia Lindenberg		
Zuordnung	Kürzel	Name
verantwortlich für	GP01	Konstruktion
verantwortlich für	A02	Outlook
verantwortlich für	A03	Delftship
verantwortlich für	C2	Client Produktion
verantwortlich für	C3	Client Produktionsleiter
hauptverantwortlich für	EG-3	Büroraum Entwicklung
Nicolas Traidl		
Zuordnung	Kürzel	Name
verantwortlich für	A02	Outlook
Anwender von	C2	Client Produktion
Anwender von	D2	Drucker Produktion
Thea Ende		
Zuordnung	Kürzel	Name
Anwender von	C2	Client Produktion
Anwender von	D2	Drucker Produktion
Heike Babik		
Zuordnung	Kürzel	Name
Anwender von	C2	Client Produktion
Anwender von	D2	Drucker Produktion
Niels Löw		
Zuordnung	Kürzel	Name
Anwender von	C2	Client Produktion
Lieselotte Hans		
Zuordnung	Kürzel	Name
verantwortlich für	A02	Outlook
verantwortlich für	C1	Client Betrieb APC
Anwender von	D1	Drucker Betrieb
hauptverantwortlich für	EG-4	Büroraum Einkauf

Kürzel	Name
Doris Richarz	
Zuordnung	Kürzel
Anwender von	C1
Anwender von	D1
Hugo Herbrand	
Zuordnung	Kürzel
Anwender von	C1
Anwender von	D1
Gisela Jacobs	
Zuordnung	Kürzel
Anwender von	C1
Anwender von	D1
Sylvia Gradl	
Zuordnung	Kürzel
verantwortlich für	GP04
verantwortlich für	A03
verantwortlich für	C2
verantwortlich für	C3
verantwortlich für	C6
Anwender von	D2
verantwortlich für	S100
verantwortlich für	S101
verantwortlich für	S102
hauptverantwortlich für	LG-1
Ralf Wanner	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2
Silvia Dohle	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2

Kürzel	Name
Lars Markus	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2
Fabio Schütz	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2
Selina Bien	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2
Gustav Borho	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2
Jule Askin	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2
Alex Reitz	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2
Lisa Strick	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2
Zacharias Michler	
Zuordnung	Kürzel
Anwender von	C2

Kürzel	Name
Zacharias Michler	
Zuordnung	Kürzel
Anwender von	D2
Phiel Wiens	
Zuordnung	Kürzel
Anwender von	C2
Anwender von	D2
Heinrich Henckel von Donnersmarck	
Zuordnung	Kürzel
verantwortlich für	GP02
verantwortlich für	GP03
verantwortlich für	A02
verantwortlich für	C1
verantwortlich für	C1
Anwender von	D1
hauptverantwortlich für	OG-1
Carmen Bell	
Zuordnung	Kürzel
Anwender von	C1
Anwender von	C1
Anwender von	D1
Mike Reichardt	
Zuordnung	Kürzel
Anwender von	C1
Anwender von	C1
Anwender von	D1
Bärbel Steuer	
Zuordnung	Kürzel
Anwender von	C1
Anwender von	D1

Kürzel	Name		
	Jason Wertenauer		
	Zuordnung	Kürzel	Name
	Anwender von	C1	Client Betrieb APC
	Anwender von	C1	Client Betrieb Laptop
	Anwender von	D1	Drucker Betrieb
Admin	Sebastian Breu		
	Zuordnung	Kürzel	Name
	verantwortlich für	GP05	Technischer Support
	Benutzer von	A01	Excel
	verantwortlich für	A02	Outlook
	verantwortlich für	A03	Delftship
	Benutzer von	A04	TeamViewer
	Benutzer von	A05	Word
	Administrator von	AP1	WLAN Access Point Produktion
	Administrator von	AP2	WLAN Access Point Betrieb
	Administrator von	C1	Client Betrieb APC
	Administrator von	C1	Client Betrieb Laptop
	Administrator von	C2	Client Produktion
	Administrator von	C3	Client Produktionsleiter
	Administrator von	C4	Client Sekretär
	Administrator von	C5	Client Geschäftsführung
	Administrator von	C6	Client CNC Fräse
	Administrator von	C7	Client Gussmaschine
	verantwortlich für	D1	Drucker Betrieb
	verantwortlich für	D2	Drucker Produktion
	Administrator von	N1	Firewall Betrieb
	Administrator von	N2	Firewall Produktion
	Administrator von	R1	Router
	Administrator von	S1	Server Betrieb
	Administrator von	S2	Server Produktion
	hauptverantwortlich für	OG-2	Büroraum IT Admin
	hauptverantwortlich für	OG-5	Serverraum

Kürzel	Name		
CEO	Ulrich Meissen		
	Zuordnung	Kürzel	Name
	Anwender von	C5	Client Geschäftsführung
	verantwortlich für	C5	Client Geschäftsführung
	hauptverantwortlich für	EG-1	Büro Raum Geschäftsleiter
CISO	Gruppe 4		
	Zuordnung	Kürzel	Name
	hauptverantwortlich für	OG-3	Büro Raum CISO
HR	Michael Holzhüter		
	Zuordnung	Kürzel	Name
	Anwender von	D1	Drucker Betrieb
	hauptverantwortlich für	EG-2	Büro Raum Personal
Sekretär	Peter Müller		
	Zuordnung	Kürzel	Name
	Anwender von	C4	Client Sekretär
	verantwortlich für	C4	Client Sekretär
	hauptverantwortlich für	EG-5	Empfang/Wartebereich

BSI IT-Grundschutz A.2 Schutzbedarfsfeststellung

Informationsverbund:	Informationsverbund
Abkürzung:	SWDS
Mitarbeiter:	35
Geltungsbereich:	Kompletter Standort der Werft
Datum:	23.01.2024, 22:13
Autor:	Gruppe 4
Version:	0.1
Freigabe:	Sebastian Breu
Vorgehensweise der Absicherung:	STANDARD

Definition der Schutzbedarfskategorien

Stufe: Unkritisch

<i>Gesetze/Vorschriften/Verträge</i>	Verstöße gegen Vorschriften und Gesetze mit keinen oder nur minimalen Konsequenzen. Keine oder nur minimale Vertragsverletzungen mit maximal geringen Konventionalstrafen.
<i>Selbstbestimmungsrecht</i>	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen nicht beeinträchtigt werden kann.
<i>persönliche Unversehrtheit</i>	Eine Beeinträchtigung ist nicht möglich.
<i>Aufgabenerfüllung</i>	Die Beeinträchtigung ist tolerabel. Die maximal tolerierbare Ausfallzeit ist größer als 72 Stunden.
<i>Innen-/Außenwirkung</i>	Es ist keine oder nur minimale Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.
<i>Finanzielle Auswirkungen</i>	Es ist kein oder nur minimaler finanzieller Schaden zu erwarten.

Stufe: Normal

<i>Gesetze/Vorschriften/Verträge</i>	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.
<i>Selbstbestimmungsrecht</i>	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
<i>persönliche Unversehrtheit</i>	Eine Beeinträchtigung erscheint nicht möglich.

Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
Innen-/Außenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel.

Stufe: Hoch	
Gesetze/Vorschriften/Verträge	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen.
Selbstbestimmungsrecht	Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
persönliche Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
Innen-/Außenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Stufe: Sehr Hoch	
Gesetze/Vorschriften/Verträge	Fundamentaler Verstoß gegen Vorschriften und Gesetze. Vertragsverletzungen, deren Haftungsschäden ruinös sind.
Selbstbestimmungsrecht	Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
persönliche Unversehrtheit	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben.
Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
Innen-/Außenwirkung	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
Finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzbedrohend.

Legende

Ableitung des Schutzbedarfs nach:

- M Maximumprinzip
- V Verteilungseffekt
- K Kumulationseffekt
- keine Ableitung

Geschäftsprozesse

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
GP01	Konstruktion	Prozess der Erstellung, Revision und Ausarbeitung der digitalen Konzeption des Bauplans von Schiffen.	Hoch Technische Details zu bestimmten Komponenten oder Systemen, die wettbewerbsrelevant sein könnten.	Hoch Technische Details von kritischer Bedeutung für die Sicherheit und Funktionalität des Schiffs.	Hoch Daten und Informationen, die für den laufenden Bauprozess von entscheidender Bedeutung sind.
GP02	Einkauf	Prozess der Materialbeschaffung für die Konstruktion und Wartung von Schiffen	Hoch Die Preisgabe der Unternehmensdaten im Bereich des Einkaufs kann zu hohen Schäden führen z.B. durch Datenschutzklagen und Ansehensverlust.	Hoch Die unbemerkte/ungewollte Veränderung von Daten des Einkaufs z.B. Bestellungen von Material kann zu hohen Schäden führen durch ausstehende Zahlungen und Vertragsstrafen.	Hoch Ein Ausfall des Prozesses länger als 5 Tage kann nicht verkraftet werden, da sonst durch die Just in Time Produktion der Produktionsprozess abbricht.
GP03	Auftragsannahme / Verkauf	Prozess der Auftragsbearbeitung.	Hoch Die Preisgabe der Unternehmensdaten im Bereich des Verkaufs kann zu hohen Schäden führen z.B. durch Datenschutzklagen, Ansehensverlust und Vertragsstrafen. Die Preisgabe der Daten aus dem technischen Support können nur begrenzten Einfluss auf das Unternehmen nehmen.	Hoch Die unbemerkte/ungewollte Veränderung von Daten des Verkaufs z.B. Bestellungen von Schiffen kann zu hohen Schäden führen durch ausstehende Zahlungen und Vertragsstrafen, Stornierungen und Ansehensverlust. Die unbemerkte/ungewollte Veränderung der Daten des technischen Supports würden zu überschaubaren Nacharbeiten und Schäden führen.	Hoch Ein Ausfall des Verkaufsprozesses kann länger als 5 Tage verkraftet werden, da der Verkauf der Produktionsware mindestens 3 Wochen vor Fertigstellung abgewickelt wird. Ein Ausfall des Prozesses länger als 5 Tage kann nicht verkraftet werden, da sonst das Risiko steigt das der Produktionsprozess stagniert.
GP04	Fertigung	Prozess der Bau und Wartung von Schiffen.	Sehr Hoch Die Preisgabe der Unternehmensgeheimnisse (z.B. Konstruktionspläne) können zu existenzbedrohenden Wettbewerbsnachteilen führen.	Sehr Hoch Die unbemerkte/ ungewollte Veränderung der Produktionsdaten z.B. Konstruktionspläne kann zu existenzbedrohenden Schäden für das Unternehmen führen.	Sehr Hoch Ein Ausfall der Produktion kann nicht über einen Zeitraum von 3 Tagen verkraftet werden und würde zu existenzbedrohenden Schäden innerhalb des Unternehmens führen.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
GP05	Technischer Support	Der Prozess für die Bereitstellung von technischer Unterstützung und Lösungen Software, Hardware oder anderen IT-bezogenen Fragen.	Hoch Wenn im technischen Support sensible Informationen behandelt werden, die nicht für unbefugte Personen zugänglich sein dürfen, wie Mitarbeiterkontaktinformation vertrauliche Support-Tickets oder technische Details zur Produktion.	Hoch Wenn die Integrität der im Support behandelten Informationen von entscheidender Bedeutung ist, um sicherzustellen, dass Kunden korrekte und verlässliche technische Unterstützung erhalten.	Hoch Da der technische Support ununterbrochen verfügbar sein muss, um Mitarbeiter bei technischen Problemen zu unterstützen. Eine Nichtverfügbarkeit könnte zu erheblichen Beeinträchtigungen führen.

Anwendungen

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
A01	Excel	Excel ermöglicht es den Mitarbeitern, umfangreiche Datenmengen aus Produktion und Vertrieb zu verarbeiten, zu analysieren und zu präsentieren. Excel wird für die Erstellung von Produktionsplänen, Verkaufsprognosen und Budgets genutzt.	Hoch Excel wird intensiv für die Verarbeitung von vertraulichen Daten im Zusammenhang mit Schiffskonstruktionen verwendet.	Hoch Die Anwendung unterstützt den Schutz vor Datenverlust oder Manipulation durch regelmäßige Backups und Sicherheitsmechanismen.	Normal Durch andere Officeprodukte (Word) kann der Auffall dieser Anwendung länger toleriert werden. Verteilungseffekt.
A02	Outlook	Outlook ermöglicht es den Mitarbeitern, E-Mails zu senden und zu empfangen, wodurch die interne und externe Kommunikation erleichtert wird.	Hoch Outlook gewährleistet die Vertraulichkeit von E-Mails durch sichere Verschlüsselung und Zugriffskontrollen. Sensible Informationen werden geschützt, um unbefugten Zugriff zu verhindern.	Hoch Die Integrität von E-Mails und Daten wird durch fortgeschrittene Sicherheitsmechanismen sichergestellt, die sicherstellen, dass Informationen während der Übertragung und Speicherung unverändert bleiben.	Hoch Outlook bietet eine hohe Verfügbarkeit, sodass Benutzer jederzeit auf ihre E-Mails, Termine und Aufgaben zugreifen können. Die Anwendung wird durch robuste Serverinfrastrukturen unterstützt.
A03	Delftship	Delftship ist eine hochentwickelte Software für den Schiffsbau, die unseren Mitarbeitern eine umfassende Plattform für die digitale Konzeption von Schiffsbauplänen bietet.	Sehr Hoch Jeglicher unberechtigter Zugriff auf diese Daten könnte zu erheblichen Sicherheitsverletzungen führen, einschließlich potenzieller Gefährdung von Geschäftsgeheimnissen und geistigem Eigentum.	Sehr Hoch Jede Manipulation oder unbefugte Änderung dieser Daten könnte schwerwiegende Auswirkungen auf die Sicherheit und Leistungsfähigkeit der hergestellten Schiffe haben.	Sehr Hoch Aufgrund der zentralen Rolle, die Delftship bei der digitalen Konzeption des Bauplans von Schiffen spielt, sind Ausfälle nicht tolerierbar.
A04	TeamViewer	Die Software ermöglicht es Benutzern, auf sichere Weise von verschiedenen Standorten aus auf Computer und andere Geräte zuzugreifen.	Hoch Unternehmens- / Personendaten könnten einsehbar sein wenn verwendet.	Normal Durch künftige Ablösung des Produkts ist kein besonderer Schutzbedarf notwendig.	Normal Durch künftige Ablösung des Produkts ist kein besonderer Schutzbedarf notwendig.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
A05	Word	Microsoft Word ist eine weit verbreitete Textverarbeitungssoftware, die von den Abteilungen Produktion und Vertrieb in unserem Unternehmen genutzt wird.	Hoch Es besteht ein Risiko des unbefugten Zugriffs auf sensible Informationen. Dies könnte zu Datenlecks, Informationsverlust und potenziell rechtlichen Konsequenzen führen, wenn vertrauliche Geschäftsinformationen in die falschen Hände geraten.	Hoch Eine Beeinträchtigung der Integrität könnte zu fehlerhaften oder manipulierten Dokumenten führen, was wiederum zu falschen Entscheidungen und geschäftlichen Unregelmäßigkeiten führen könnte.	Normal Ein Ausfall des Prozesses länger als 5 Tage kann nicht verkraftet werden, da sonst das Risiko steigt das der Produktionsprozess stagniert.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
AP1	WLAN Access Point Produktion		Normal Schutz interner Netzwerkinformationen im Bürobereich.	Hoch Sicherstellung ordnungsgemäßer Kommunikation im Bürobereich.	Hoch Sicherstellung einer kontinuierlichen Nutzung des Büro-WLANS.
AP2	WLAN Access Point Betrieb		Normal Schutz interner Netzwerkinformationen im Bürobereich.	Hoch Sicherstellung ordnungsgemäßer Kommunikation im Bürobereich.	Hoch Sicherstellung einer kontinuierlichen Nutzung des Büro-WLANS.
C1	Client Betrieb APC		Hoch Vererbung	Hoch Vererbung	V Normal Es gibt mehrere Clients, deswegen kann der Ausfall einer gewissen Anzahl verkraftet werden.
C1	Client Betrieb Laptop		Hoch Vererbung	Hoch Vererbung	V Normal Es gibt mehrere Clients, deswegen kann der Ausfall einer gewissen Anzahl verkraftet werden.
C2	Client Produktion		Sehr Hoch Vererbung	Sehr Hoch Vererbung	V Normal Es gibt mehrere Clients, deswegen kann der Ausfall einer gewissen Anzahl verkraftet werden.
C3	Client Produktionsleiter		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
C4	Client Sekretär		Hoch Die Vertraulichkeit ist von entscheidender Bedeutung, da der Client wahrscheinlich sensible Informationen und Dokumente enthält. Der Zugriff sollte auf autorisierte Benutzer beschränkt sein, um den Schutz vertraulicher Daten sicherzustellen.	Hoch Die Integrität des Clients ist entscheidend, um sicherzustellen, dass die auf dem Computer gespeicherten Dokumente und Informationen korrekt und unverändert bleiben. Manipulationen könnten zu falschen Informationen und Sicherheitsproblemen führen.	Hoch Die Verfügbarkeit des Sekretär-Clients ist wichtig, um sicherzustellen, dass der Sekretär effizient arbeiten kann. Ausfälle könnten zu Arbeitsunterbrechungen und -verzögerungen führen.
C5	Client Geschäftsführung		Sehr Hoch Der Client des Geschäftsführers enthält äußerst vertrauliche Informationen, wie Geschäftsstrategien, Finanzdaten und möglicherweise personenbezogene Daten. Der Zugriff sollte auf die höchsten Berechtigungsstufen beschränkt sein, um unbefugten Zugriff zu verhindern.	Hoch Die Integrität der auf diesem Client gespeicherten Daten ist von entscheidender Bedeutung, um sicherzustellen, dass geschäftskritische Informationen nicht manipuliert oder verfälscht werden.	Hoch Die Verfügbarkeit dieses Clients ist wichtig, um sicherzustellen, dass der Geschäftsführer jederzeit auf relevante Informationen zugreifen kann. Ausfälle könnten die Effizienz und Reaktionsfähigkeit des Managements beeinträchtigen und sollten daher vermieden werden.
C6	Client CNC Fräse		Hoch Vererbung	Hoch Vererbung	Hoch Die Verfügbarkeit der Clients ist von entscheidender Bedeutung, um einen reibungslosen Produktionsprozess sicherzustellen. Ausfälle könnten zu Produktionsverzögerungen und -ausfällen führen.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
C7	Client Gussmaschine		Hoch Vererbung	Hoch Vererbung	Sehr Hoch Die Verfügbarkeit der Clients ist von entscheidender Bedeutung, um einen reibungslosen Produktionsprozess sicherzustellen. Ausfälle könnten zu Produktionsverzögerungen und -ausfällen führen.
D1	Drucker Betrieb		Normal Drucker speichern normalerweise keine hochsensiblen Informationen.	Normal Die Integrität des Druckers bezieht sich darauf, dass er korrekte und unveränderte Druckaufträge ausführt. Manipulationen am Drucker könnten zu Fehldrucken oder unberechtigten Zugriffen auf Druckaufträge führen.	Hoch Die Verfügbarkeit des Druckers ist wichtig für den reibungslosen Geschäftsbetrieb. Ein Ausfall des Druckers könnte zu Verzögerungen in der Dokumentenverarbeitung führen.
D2	Drucker Produktion		Normal Produktionsdrucker in der Regel sind eher auf die Ausgabe von Produktionsdokumenten ausgerichtet, die normalerweise nicht als vertraulich gelten.	Normal Die Integrität ist wichtig, um sicherzustellen, dass Produktionsdokumente korrekt und unverändert ausgedruckt werden.	Hoch Die Verfügbarkeit des Produktionsdruckers ist entscheidend für einen effizienten Produktionsprozess. Ein Ausfall könnte zu Produktionsverzögerungen führen.
HP1	Switch Betrieb		Hoch Vererbung	Hoch Vererbung	K Sehr Hoch Sicherstellung einer kontinuierlichen Büronetzwerknutzung.
HP2	Switch Produktion		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Gewährleistung kontinuierlicher und zuverlässiger Produktionsabläufe.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit		Schutzbedarf Integrität		Schutzbedarf Verfügbarkeit	
N1	Firewall Betrieb		K	Sehr Hoch Da fast alle Anwendungen, sowie der DNS-Server, die Active Directory und der Webserver auf dem Server laufen, der die Verbindung zur Firewall hat.	K	Sehr Hoch Gewährleistung ordnungsgemäßer Firewall-Funktionen.	K	Sehr Hoch Kontinuierlicher Schutz vor unbefugtem Zugriff.
N2	Firewall Produktion			Sehr Hoch Da fast alle Anwendungen, sowie der DNS-Server, die Active Directory und der Webserver auf dem Server laufen, der die Verbindung zur Firewall hat.		Sehr Hoch Gewährleistung ordnungsgemäßer Firewall-Funktionen.		Sehr Hoch Kontinuierlicher Schutz vor unbefugtem Zugriff.
R1	Router			Hoch Vererbung		Hoch Vererbung		Hoch Vererbung
S1	Server Betrieb			Hoch Vererbung		Hoch Vererbung	K	Sehr Hoch Kummulationseffekt da fast alle Anwendungen, sowie der DNS-Server, die Active Directory und der Webserver auf dem Server laufen.
S2	Server Produktion			Sehr Hoch Vererbung		Sehr Hoch Vererbung		Sehr Hoch Vererbung

ICS-Syteme

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
S100	SPS	Die SPS spielt eine entscheidende Rolle bei der Überwachung und Steuerung von Maschinen, Förderbändern und anderen produktionsrelevanten Abläufen.	Hoch Ein unbefugter Zugriff auf die SPS-Programmierung könnte zwar potenzielle Sicherheitsprobleme verursachen, ist jedoch in der Regel weniger kritisch als bei anderen Anwendungen.	Sehr Hoch Eine Beeinträchtigung der Integrität könnte zu schwerwiegenden Fehlfunktionen in der Produktionsanlage führen, was wiederum zu Qualitätsproblemen, Produktionsausfällen und Sicherheitsrisiken führen könnte.	Sehr Hoch Eine kontinuierliche Verfügbarkeit ist entscheidend, um einen reibungslosen Betrieb der Produktionsanlagen zu gewährleisten und Ausfallzeiten zu minimieren.
S101	Produktionsmaschine - CNC Fräse	Die CNC Fräse wird für die Herstellung von präzisen Bauteilen und Werkstücken aus verschiedenen Materialien wie Metall, Kunststoff oder Holz benutzt.	Hoch Der Zugriff auf die programmierbaren Codes und Designdaten muss auf autorisiertes Personal beschränkt sein, um die Integrität der Produktion und die geistigen Eigentumsrechte zu schützen.	Hoch Jegliche unbeabsichtigten oder böswilligen Änderungen an den Produktionscodes könnten zu fehlerhaften Produkten führen und müssen daher streng kontrolliert werden.	Sehr Hoch In kontinuierlicher Betrieb ist entscheidend, um Produktionsziele zu erreichen. Regelmäßige Wartung und sofortige Behebung von Störungen sind notwendig, um die Ausfallzeit zu minimieren.
S102	Produktionsmaschine - Gussmaschine		Hoch Der Zugang zu den spezifischen Gussparametern sollte beschränkt sein, um die Integrität der Gussproduktion zu wahren.	Hoch Jede Veränderung an den Gussparametern oder der Schmelztemperatur könnte die Qualität der produzierten Gussteile beeinträchtigen und muss daher streng überwacht werden.	Sehr Hoch Kontinuierlicher Betrieb und schnelle Reaktion auf Störungen sind entscheidend, um die Produktion effizient zu gestalten und Liefertermine einzuhalten.

Anderes / IoT-Systeme

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
I1	Videoüberwachung		Hoch Daten können Informationen über Personen enthalten deshalb besonders Schützenswert	Hoch Änderung der Daten kann eine Straftat z.B. Diebstahl von Betriebsmitteln verschleichern	Normal Verteilungseffekt da es mehrere Kameras gibt kann der Ausfall einer gewissen Anzahl über einen kurzen Zeitraum verkraftet werden.
K1	Kaffeemaschine		Unkritisch Keine relevanten vertraulichen Informationen.	Unkritisch Geringe Auswirkung auf den Geschäftsbetrieb bei Ausfall oder Störungen.	Unkritisch Beeinflusst den Betrieb im Bürobereich, aber nicht kritisch für die Produktion.

Kommunikationsverbindungen

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
AP1<N	WLAN AP Betrieb<>Firewall Betrieb		Normal Vererbung	Normal Vererbung	Hoch Hoch
AP2<N	WLAN AP Produktion<>Firewa Produktion		Normal Vererbung	Normal Vererbung	Hoch Vererbung
C1/4/5<	Client Betrieb<>WLAN AP Betrieb		Normal Vererbung	Hoch Vererbung	Hoch Vererbung
C1/4/5<	Client Betrieb<>Firewall Betrieb		Hoch Vererbung	Hoch Vererbung	Hoch Verebung
C1<C2	Client Betrieb<>Client Produktion		Hoch Vererbung	Hoch Vererbung	Normal Vererbung
C1<C4	Client Betrieb<>Client Sekretär		Hoch Vererbung	Hoch Vererbung	Normal Vererbung
C1<C5	Client Betrieb<>Client Geschäftsführung		Hoch Vererbung	Hoch Vererbung	Hoch Vererbung
C1<D1	Client Betrieb<>Drucker Betrieb		Normal Vererbung	Normal Vererbung	Normal Vererbung
C1<S1	Client Betrieb<>Server Betrieb		Hoch Vererbung	Hoch Vererbung	K Hoch Vererbung
C2/3/6/7	Client Produktion<>WLAN AP Produktion		Normal Vererbung	Hoch Vererbung	Hoch Vererbung
C2/3<S S101/10	Client Produktion/ Produktionsleiter<> Systeme		Hoch Vererbung	Hoch Vererbung	Sehr Hoch Vererbung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
C2/C3/ C6/ C7↔N2	Client Produktion↔Firewa Produktion		Hoch Vererbung	Hoch Vererbung	Hoch Vererbung
C2↔C3	Client Produktion↔Client Produktionsleiter		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung
C2↔C6	Client Produktion↔Client CNC Fräse		Hoch Vererbung	Hoch Vererbung	Hoch Vererbung
C2↔C7	Client Produktion↔Client Gussmaschine		Hoch Vererbung	Hoch Vererbung	Sehr Hoch Vererbung
C2↔D2	Client Produktion↔Drucke Produktion		Normal Vererbung	Normal Vererbung	Hoch Vererbung
C2↔S2	Client Produktion↔Server Produktion		Sehr Hoch Da es sich um den Kernprozess der Werft handelt, ist die ordnungsgemäße und sichere Übertragung von Daten zwischen dem Produktionsclient und dem Produktionsserver entscheidend für die reibungslose Durchführung der Produktion von Schiffen.	Sehr Hoch Eine fehlerhafte Integrität könnte zu Produktionsfehlern oder Sicherheitsrisiken führen.	Sehr Hoch Jeder Ausfall oder jede Beeinträchtigung der Verfügbarkeit könnte zu erheblichen Produktionsverzögerungen führen.
C3↔D2	Client Produktionsleiter↔[Produktion		Normal Vererbung	Normal Vererbung	Hoch Vererbung
C4↔C5	Client Sekretär↔Client Geschäftsführung		Hoch Vererbung	Hoch Vererbung	Hoch Vererbung
C4↔D1	Client Sekräter↔Drucker Betrieb		Normal Vererbung	Normal Vererbung	Hoch Vererbung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
C5<D1	Client Geschäftsleitung< Betrieb		Normal Vererbung	Normal Vererbung	Hoch Vererbung
HP1<A	Switch Betrieb<WLAN AP Betrieb		Normal Vererbung	Hoch Vererbung	Hoch Vererbung
HP1<C	Switch Betrieb<Client Betrieb		Hoch Vererbung	Hoch Vererbung	Sehr Hoch Vererbung
HP1<D	Switch Betrieb<Drucker Betrieb		Normal Vererbung	Normal Vererbung	Hoch Vererbung
HP1<N	Server Betrieb<Firewall Betrieb		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung
HP1<S	Switch Betrieb<Server Betrieb		Hoch Vererbung	Hoch Vererbung	Sehr Hoch Vererbung
HP2->AP1	Switch Produktion<WLAN AP Produktion		Normal Vererbung	Hoch Vererbung	Hoch Vererbung
HP2<C	Switch Produktion<Client Produktion		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung
HP2<N	Switch Betrieb<Firewall Betrieb		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung
HP2<S	Switch Produktion<Drucker Produktion		Normal Vererbung	Normal Vererbung	Hoch Vererbung
HP2<S	Switch Produktion<Server Produktion		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
K40	Firewall Prod <>> Router		Hoch Der Schutz vor unbefugtem Zugriff auf diese Informationen ist entscheidend für die Sicherheit des Netzwerks.	Hoch Eine hohe Integrität schützt vor unautorisierten Änderungen, die die Netzwerksicherheit beeinträchtigen könnten.	Sehr Hoch Die Verfügbarkeit dieser Verbindung ist von entscheidender Bedeutung, da sie einen zentralen Punkt für die Netzwerkkommunikation darstellt.
K42	Router<>Videoüberwachungskamera		Hoch Die Videoüberwachungskameras können sensible Bilder und Videos aufzeichnen.	Hoch Die Integrität der aufgezeichneten Videodateien ist wichtig, um sicherzustellen, dass die Informationen nicht manipuliert oder gefälscht werden	V Normal Jede Unterbrechung könnte zu Sicherheitslücken führen.
K43	Router<>Internet		Hoch Die Vertraulichkeit der Daten zwischen dem Router und dem Internet ist wichtig, um sensible Informationen vor unbefugtem Zugriff zu schützen.	Hoch Die Integrität der Daten ist entscheidend, um sicherzustellen, dass die Informationen während der Übertragung nicht manipuliert oder verändert werden.	Sehr Hoch Die Verfügbarkeit ist von höchster Bedeutung, da eine kontinuierliche Verbindung zwischen dem Router und dem Internet sicherstellen muss, dass die Benutzer jederzeit auf die benötigten Ressourcen zugreifen können.
K44	Kaffeemaschine <>> WLAN AP PROD		Unkritisch Spielt keine entscheidende Rolle.	Unkritisch Spielt keine entscheidende Rolle.	Unkritisch Spielt keine entscheidende Rolle.
K45	Firewall Betrieb<->Router		Hoch Die Kommunikation zwischen Firewall und Router enthält sensible Informationen über die Netzwerkkonfiguration und Sicherheitsrichtlinien.	Hoch Die Integrität der Kommunikation zwischen Firewall Betrieb und Router ist von entscheidender Bedeutung.	Hoch Die ständige Verfügbarkeit der Kommunikation zwischen Firewall Betrieb und Router ist wesentlich für einen reibungslosen Netzwerkbetrieb.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
K46	Firewall Betrieb<>Firewall Produktion		Hoch Zwischen den Firewalls werden sensible Sicherheitsinformationen ausgetauscht.	Hoch Die Integrität ist ebenfalls hoch, um sicherzustellen, dass keine unbefugten Änderungen an den Sicherheitsregeln oder -einstellungen vorgenommen werden.	Sehr Hoch Die Verfügbarkeit ist entscheidend, da eine unterbrochene Kommunikation zwischen den Firewalls schwerwiegende Auswirkungen auf die Sicherheit des Netzwerks haben kann.
S1<>N1	Server Betrieb<>Firewall Produktion		Hoch Die Verbindung zwischen Server und Firewall enthält sensible Informationen.	Hoch Es ist wichtig sicherzustellen, dass die Informationen, die die Firewall passieren, nicht manipuliert werden.	Unbearbeitet Ausfälle könnten zu Sicherheitslücken führen.
S1<>S2	Server Betrieb<>Server Produktion		Hoch Die sensible Informationen werden zwischen den Servern übertragen.	Hoch Die Daten zwischen den Servern sollen korrekt und unverändert übertragen werden.	Hoch Die Verbindung zwischen den Servern ist geschäftskritisch und Ausfälle müssen vermieden werden.
S2<>N2	Server Produktion<>Firewa Produktion		Hoch Die Verbindung zwischen Server und Firewall enthält sensible Informationen.	Hoch Es ist wichtig sicherzustellen, dass die Informationen, die die Firewall passieren, nicht manipuliert werden.	Hoch Ausfälle könnten zu Sicherheitslücken führen.

Räume

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit		Schutzbedarf Integrität		Schutzbedarf Verfügbarkeit	
	Halle und Materiallager		M	Sehr Hoch	M	Sehr Hoch	M	Sehr Hoch
EG-1	Büro Raum Geschäftsführer		Hoch Das Büro des Geschäftsführers enthält vertrauliche Geschäftsinformationen, wie strategische Pläne, finanzielle Daten, Verträge und personenbezogene Informationen. Der Schutz dieser Informationen ist entscheidend, um unautorisierten Zugriff und potenzielle Datenschutzverletzungen zu verhindern.	Hoch Die Integrität der Informationen im Büro des Geschäftsführers ist von grundlegender Bedeutung, um sicherzustellen, dass keine unbefugten Änderungen oder Manipulationen an strategischen Dokumenten, Verträgen und anderen geschäftskritischen Unterlagen vorgenommen werden.	Hoch Die Verfügbarkeit der Informationen im Büro des Geschäftsführers ist entscheidend für effektive Entscheidungsfindung und Geschäftsführung.			
EG-2	Büro Raum Personal		Sehr Hoch Der Büror Raum für HR enthält hochsensible personenbezogene Daten, wie Mitarbeiterverträge, Gehaltsinformationen, Leistungsbeurteilungen und möglicherweise auch Informationen zu Mitarbeitergesundheit und -qualifikationen.	Hoch Die Integrität der HR-Daten ist entscheidend, um sicherzustellen, dass die Informationen genau, konsistent und vollständig sind.	Hoch Die Verfügbarkeit von HR-Informationen ist wichtig, um eine effiziente Personalarbeit zu gewährleisten.			

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit		Schutzbedarf Integrität		Schutzbedarf Verfügbarkeit	
EG-3	Büro Raum Entwicklung		Hoch Der Büro Raum enthält hochsensible Konstruktionspläne und technische Zeichnungen für Schiffe. Diese Pläne können geistiges Eigentum, Patente und fortgeschrittene technische Informationen enthalten, die von strategischer Bedeutung für das Unternehmen sind.		Hoch Die Integrität der Schiffspläne ist von höchster Wichtigkeit, um sicherzustellen, dass die Konstruktionsinformationen korrekt und unverändert bleiben.		Hoch Die Verfügbarkeit der Schiffspläne ist für den reibungslosen Fortschritt der Entwicklungsarbeit entscheidend. Der Büro Raum sollte so gestaltet sein, dass Entwickler jederzeit Zugriff auf ihre Arbeitsunterlagen haben, um effizient und zeitnah arbeiten zu können.	
EG-4	Büro Raum Einkauf		Hoch Der Büro Raum enthält vertrauliche Informationen über Schiffsdetails und Einkaufsaktivitäten, darunter möglicherweise Preisverhandlungen, Lieferantenverträge und andere geschäftskritische Informationen.		Hoch Die Integrität der Informationen im Zusammenhang mit Schiffsdetails und Teilebeschaffung ist von entscheidender Bedeutung, um sicherzustellen, dass die beschafften Produkte den erforderlichen Standards entsprechen und keine Risiken für die Schiffskonstruktion darstellen.		Hoch Die Verfügbarkeit von Schiffsdetails und Teileinformationen ist entscheidend für den reibungslosen Ablauf der Beschaffungsaktivitäten. Der Büro Raum sollte so gestaltet sein, dass das Einkaufsteam jederzeit auf die benötigten Unterlagen zugreifen kann, um effiziente und zeitnahe Entscheidungen zu treffen.	
EG-5	Empfang/ Wartebereich		M	Unbearbeitet	M	Unbearbeitet	M	Unbearbeitet
EG-6	Küche		M	Unkritisch	M	Unkritisch	M	Unkritisch

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
LG-1	Büro Raum Produktion		Hoch Das Büro enthält vertrauliche Informationen über Produktionspläne, Technologien, Konstruktionszeichnungen und möglicherweise auch Informationen zu Materialbeschaffung und Herstellungsprozessen.	Hoch Die Integrität von Produktionsplänen und Konstruktionszeichnungen ist unerlässlich, um sicherzustellen, dass die hergestellten oder reparierten Schiffe den erforderlichen Standards entsprechen.	Hoch Die Verfügbarkeit ist entscheidend für einen effizienten Ablauf der Schiffsbau- und Reparaturprozesse. Das Büro sollte so gestaltet sein, dass die Produktionsmitarbeiter jederzeit auf die benötigten Informationen zugreifen können, um den Bau oder die Reparatur von Schiffen effektiv zu leiten.
LG-2	Küche		M Unbearbeitet	M Unbearbeitet	M Unbearbeitet
OG-1	Büro Raum Vertrieb		Hoch Der Büror Raum enthält hochvertrauliche Kundendaten, einschließlich persönlicher Informationen, Verträge, Bestellungen und finanzieller Angaben. Die Vertraulichkeit ist von höchster Bedeutung, um den Schutz der Kunden und die Einhaltung datenschutzrechtlicher Bestimmungen sicherzustellen.	Hoch Die Integrität von Kundenaufträgen und -daten ist entscheidend, um sicherzustellen, dass Transaktionen genau und zuverlässig abgewickelt werden.	Hoch Die Verfügbarkeit von Kundenaufträgen und -daten ist entscheidend für die reibungslose Abwicklung von Verkaufsaktivitäten und Kundenservice. Der Büror Raum sollte so gestaltet sein, dass das Vertriebsteam jederzeit auf die benötigten Informationen zugreifen kann, um Kundenanfragen zu bearbeiten und Bestellungen effizient zu verwalten.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit		Schutzbedarf Integrität		Schutzbedarf Verfügbarkeit	
OG-2	Büro Raum IT Admin		Hoch Das Büro des IT-Administrators enthält vertrauliche Informationen über Sicherheitsrichtlinien, Zugangsberechtigungen und Passwörter.		Hoch Die Integrität von IT-Konfigurationen und -Daten ist unerlässlich, um sicherzustellen, dass das Netzwerk stabil und sicher bleibt.		Hoch Die Verfügbarkeit des IT-Administrators ist entscheidend für den reibungslosen Betrieb der IT-Infrastruktur. Das Büro sollte so gestaltet sein, dass der Administrator jederzeit auf notwendige Tools, Dokumentationen und Ressourcen zugreifen kann, um Probleme schnell zu identifizieren und zu lösen.	
OG-3	Büro Raum CISO		Hoch Das Büro des IT-Sicherheitsbeauftragten enthält hochvertrauliche Informationen über Sicherheitsrichtlinien, Schwachstellenanalysen, Incident-Response-Pläne und andere sensible Sicherheitsdokumentationen.		Hoch Die Integrität von Sicherheitsrichtlinien, Berichten und Analysen ist wesentlich, um sicherzustellen, dass die Sicherheitsstrategie konsistent und effektiv bleibt.		Hoch Die Verfügbarkeit des IT-Sicherheitsbeauftragten ist entscheidend für eine schnelle Reaktion auf Sicherheitsvorfälle und die laufende Überwachung der Sicherheitslage. Das Büro sollte so gestaltet sein, dass der Sicherheitsbeauftragte jederzeit auf notwendige Ressourcen, Berichte und Sicherheitswerkzeuge zugreifen kann.	
OG-4	Pausenraum		M	Unbearbeitet	M	Unbearbeitet	M	Unbearbeitet
OG-5	Serverraum		M	Sehr Hoch	M	Sehr Hoch	M	Sehr Hoch

Informationsverbund:	Informationsverbund
Abkürzung:	SWDS
Mitarbeiter:	35
Geltungsbereich:	Kompletter Standort der Werft
Datum:	23.01.2024, 22:14
Autor:	Gruppe 4
Version:	0.1
Freigabe:	Sebastian Breu
Vorgehensweise der Absicherung:	STANDARD

Übersicht: Liste verwendeter Bausteine

Baustein	Name	Anzahl Zuordnungen
ORP.3	Sensibilisierung und Schulung zur Informationssicherheit	1
CON.6	Löschen und Vernichten	1
CON.9	Informationsaustausch	1
OPS.1.2.5	Fernwartung	1
DER.4	Notfallmanagement	1
APP.1.1	Office-Produkte	2
SYS.1.1	Allgemeiner Server	2
SYS.1.2.3	Windows Server	2
SYS.3.1	Laptops	1
NET.3.1	Router und Switches	3
INF.7	Büroarbeitsplatz	9

Informationsverbund

ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

Beschreibung:

Bearbeitungsreihenfolge: R1

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Verantwortlicher: Breu, Sebastian

CON.6 Löschen und Vernichten

Beschreibung:

Bearbeitungsreihenfolge: R1

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Verantwortlicher: Breu, Sebastian

CON.9 Informationsaustausch

Beschreibung:

Bearbeitungsreihenfolge: R3

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

DER.4 Notfallmanagement

Beschreibung:

Bearbeitungsreihenfolge: R3

Letzte Änderung: 01.02.2023

Hauptverantwortlicher: Meissen, Ulrich

grundsätzlich zuständig:, Gruppe 4

Verantwortlicher: Breu, Sebastian

Geschäftsprozesse

GP01 Konstruktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

GP02 Einkauf

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

GP03 Auftragsannahme / Verkauf

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

GP04 Fertigung

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

GP05 Technischer Support

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

Anwendungen

A01 Excel

APP.1.1 Office-Produkte

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

A02 Outlook

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

A03 Delftship

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

A04 TeamViewer

OPS.1.2.5 Fernwartung

Beschreibung:

Bearbeitungsreihenfolge: R3

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

A05 Word

APP.1.1 Office-Produkte

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

IT-Systeme

AP1 WLAN Access Point Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

AP2 WLAN Access Point Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C1 Client Betrieb Laptop

SYS.3.1 Laptops

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C1 Client Betrieb APC

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C2 Client Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C3 Client Produktionsleiter

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C4 Client Sekretär

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C5 Client Geschäftsführung

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C6 Client CNC Fräse

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C7 Client Gussmaschine

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

D1 Drucker Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

D2 Drucker Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP1 Switch Betrieb

NET.3.1 Router und Switches

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP2 Switch Produktion

NET.3.1 Router und Switches

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

N1 Firewall Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

N2 Firewall Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

R1 Router

NET.3.1 Router und Switches

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

S1 Server Betrieb

SYS.1.1 Allgemeiner Server

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

SYS.1.2.3 Windows Server

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

S2 Server Produktion

SYS.1.1 Allgemeiner Server

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

SYS.1.2.3 Windows Server

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

ICS-Systeme

S100 SPS

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

S101 Produktionsmaschine - CNC Fräse

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

S102 Produktionsmaschine - Gussmaschine

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

Anderes / IoT-System

I1 Videoüberwachung

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

K1 Kaffeemaschine

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

Kommunikationsverbindungen

AP1<>>N1 WLAN AP Betrieb<>>Firewall Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

AP2<>>N2 WLAN AP Produktion<>>Firewall Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C1/4/5<>>AI Client Betrieb<>>WLAN AP Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C1/4/5<>>N1 Client Betrieb<>>Firewall Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C1<>>C2 Client Betrieb<>>Client Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C1<>>C4 Client Betrieb<>>Client Sekretär

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C1<>>C5 Client Betrieb<>>Client Geschäftsführung

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C1<>>D1 Client Betrieb<>>Drucker Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C1<>>S1 Client Betrieb<>>Server Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C2/3/6/7<>> Client Produktion<>>WLAN AP Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C2/3<>>S10 Client Produktion/Produktionsleiter<>>ICS-Systeme

S101/102

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C2/C3/C6/ Client Produktion<>>Firewall Produktion

C7<>>N2

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C2<>C3 Client Produktion<>Client Produktionsleiter

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C2<>C6 Client Produktion<>Client CNC Fräse

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C2<>C7 Client Produktion<>Client Gussmaschine

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C2<>D2 Client Produktion<>Drucker Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C2<>S2 Client Produktion<>Server Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C3<>D2 Client Produktionsleiter<>Drucker Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C4<>>C5 Client Sekretär<>>Client Geschäftsführung

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C4<>>D1 Client Sekräter<>>Drucker Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

C5<>>D1 Client Geschäftsführung<>>Drucker Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP1<>>AP2 Switch Betrieb<>>WLAN AP Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP1<>>C1/4 Switch Betrieb<>>Client Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP1<>>D1 Switch Betrieb<>>Drucker Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP1<>N1 Server Betrieb<>Firewall Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP1<>S1 Switch Betrieb<>Server Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP2<->AP1 Switch Produktion<>WLAN AP Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP2<>C2/3 Switch Produktion<>Client Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP2<>N2 Switch Betrieb<>Firewall Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP2<>S2 Switch Produktion<>Drucker Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

HP2<>S2 Switch Produktion<>Server Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

K40 Firewall Prod <> Router

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

K42 Router<>Videoüberwachung

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

K43 Router<>Internet

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

K44 Kaffeemaschine <> WLAN AP PROD

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

K45 Firewall Betrieb<->Router

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

K46 Firewall Betrieb<>Firewall Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

S1<>N1 Server Betrieb<>Firewall Betrieb

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

S1<>S2 Server Betrieb<>Server Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

S2<>N2 Server Produktion<>Firewall Produktion

Beschreibung:

Bearbeitungsreihenfolge:

Letzte Änderung:

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

Räume

EG-1 Büroraum Geschäftsleiter

INF.7 Büroarbeitsplatz

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

EG-2 Büroraum Personal

INF.7 Büroarbeitsplatz

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

EG-3 Büroraum Entwicklung

INF.7 Büroarbeitsplatz

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

EG-4 Büroraum Einkauf

INF.7 Büroarbeitsplatz

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

OG-1 Büroraum Vertrieb

INF.7 Büroarbeitsplatz

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

OG-2 Büroraum IT Admin

INF.7 Büroarbeitsplatz

Beschreibung:

Bearbeitungsreihenfolge: R2

Letzte Änderung: 01.02.2023

Grundsätzlich zuständig:

Weitere Zuständigkeiten:

OG-3	Büroraum CISO
INF.7	Büroarbeitsplatz
Beschreibung:	
Bearbeitungsreihenfolge: R2	
Letzte Änderung: 01.02.2023	
Grundsätzlich zuständig:	
Weitere Zuständigkeiten:	
EG-5	Empfang/Wartebereich
Beschreibung:	
Bearbeitungsreihenfolge:	
Letzte Änderung:	
Grundsätzlich zuständig:	
Weitere Zuständigkeiten:	
EG-6	Küche
Beschreibung:	
Bearbeitungsreihenfolge:	
Letzte Änderung:	
Grundsätzlich zuständig:	
Weitere Zuständigkeiten:	
OG-4	Pausenraum
Beschreibung:	
Bearbeitungsreihenfolge:	
Letzte Änderung:	
Grundsätzlich zuständig:	
Weitere Zuständigkeiten:	
OG-5	Serverraum
Beschreibung:	
Bearbeitungsreihenfolge:	
Letzte Änderung:	
Grundsätzlich zuständig:	
Weitere Zuständigkeiten:	
Halle und Materiallager	
Beschreibung:	
Bearbeitungsreihenfolge:	
Letzte Änderung:	
Grundsätzlich zuständig:	
Weitere Zuständigkeiten:	

LG-1 Büroraum Produktion

INF.7 Büroarbeitsplatz

Beschreibung:**Bearbeitungsreihenfolge:** R2**Letzte Änderung:** 01.02.2023**Grundsätzlich zuständig:****Weitere Zuständigkeiten:****LG-2 Küche****Beschreibung:****Bearbeitungsreihenfolge:****Letzte Änderung:****Grundsätzlich zuständig:****Weitere Zuständigkeiten:**

Informationsverbund:	Informationsverbund
Abkürzung:	SWDS
Mitarbeiter:	35
Geltungsbereich:	Kompletter Standort der Werft
Datum:	23.01.2024, 22:16
Autor:	Gruppe 4
Version:	0.1
Freigabe:	Sebastian Breu
Vorgehensweise der Absicherung:	STANDARD

Informationsverbund

SWDS	Informationsverbund
ORP.3	Sensibilisierung und Schulung zur Informationssicherheit
Beschreibung:	
Verantwortlicher:	Breu, Sebastian
ORP.3.A1	Sensibilisierung der Institutionsleitung für Informationssicherheit [Vorgesetzte, Institutionsleitung]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	30 Minuten Schulung ist nicht genug - der Inhalt ist auch allgemein und nicht spezifiziert.
ORP.3.A3	Einweisung des Personals in den sicheren Umgang mit IT [Vorgesetzte, Personalabteilung, IT-Betrieb]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	30 Minuten Schulung ist nicht genug - der Inhalt ist auch allgemein und nicht spezifiziert.
ORP.3.A4	Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt eine Schulung von 30 Minuten welche aber keinem klaren Konzept folgt.
ORP.3.A6	Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	30 Minuten Schulung einmal pro Jahr findet statt.

ORP.3.A7	Schulung zur Vorgehensweise nach IT-Grundschutz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Die Schulungen werden auf der Privatbasis durchgeführt.
ORP.3.A8	Messung und Auswertung des Lernerfolgs [Personalabteilung]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Messung und Auswertung des Lernerfolgs.
CON.6	Löschen und Vernichten
Beschreibung:	
Verantwortlicher:	Breu, Sebastian
CON.6.A1	Regelung für die Löschung und Vernichtung von Informationen [Zentrale Verwaltung, Fachverantwortliche, Datenschutzbeauftragte, IT-Betrieb]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Es wird evtl. ein veraltetes Konzept für die Überschreibung benutzt.
CON.6.A2	Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Die Daten werden durch löscherfahren vernichtet, aber papier etc nicht.
CON.6.A4	Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Es gibt keine geeignete Geräte und Werkzeuge für die Löschung alle eingesetzten Datenträgerarten.
CON.6.A8	Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen [Mitarbeitende, IT-Betrieb, Datenschutzbeauftragte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Der System Administratot macht das mit Hilfe eines freeware tools.

CON.6.A11	Löschen und Vernichtung von Datenträgern durch externe Dienstleistende
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keinen Prozess zum Löschen und Vernichten durch externe Dienstleistende.
CON.6.A12	Mindestanforderungen an Verfahren zur Lösung und Vernichtung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	
CON.6.A13	Vernichtung defekter digitaler Datenträger
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Erfolgt durch sichere Beseitigung vom Admin.
CON.9	Informationsaustausch
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
CON.9.A1	Festlegung zulässiger Empfänger [Zentrale Verwaltung]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Sicherstellung, dass es durch die Weitergabe von Informationen nicht gegen rechtliche Rahmenbedingungen verstößen wird.
CON.9.A2	Regelung des Informationsaustausches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Der CEO hat dies entschieden, aber eher so in einer großen Gruppenleiterrunde. Allgemeiner Konsens ist, das keiner Informationen nach draußen geben darf, es sei denn der CEO erlaubt es.
CON.9.A3	Unterweisung des Personals zum Informationsaustausch [Fachverantwortliche]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Fachverantwortliche informieren die Mitarbeitenden über die Rahmenbedingungen jedes Informationsaustauschs nicht.

CON.9.A4	Vereinbarungen zum Informationsaustausch mit Externen [Zentrale Verwaltung]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Bei einem regelmäßigen Informationsaustausch mit anderen Institutionen vereinbart die Institution die Rahmenbedingungen für den Informationsaustausch formal nicht.
CON.9.A5	Beseitigung von Restinformationen vor Weitergabe [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Es wird teilweise über die Gefahren von Rest- und Zusatzinformationen in Dokumenten und Dateien vom Admin informiert.
CON.9.A6	Kompatibilitätsprüfung des Sende- und Empfangssystems
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Vor einem Informationsaustausch wird überprüft, dass die eingesetzten IT-Systeme und Produkte kompatibel sind. (alles was es an boardmittel gibt)
CON.9.A7	Sicherungskopie der übermittelten Daten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Eine Sicherungskopie der übermittelten Informationen wird angefertigt (Backup).
CON.9.A8	Verschlüsselung und digitale Signatur
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Informationen werden während des Austausches kryptografisch durch Transportverschlüsselung gesichert.
DER.4	Notfallmanagement
Beschreibung:	
Hauptverantwortlicher:	Meissen, Ulrich
Verantwortlicher:	Breu, Sebastian
grundätzlich zuständig	Gruppe 4

DER.4.A1	Erstellung eines Notfallhandbuchs
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Das Notfallhandbuch wurde in Papierform und digital erstellt.
DER.4.A2	Integration von Notfallmanagement und Informationssicherheitsmanagement [Informationssicherheitsbeauftragte (ISB)]

Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es besteht die Notwendigkeit, die Integration und Koordination dieser beiden Managementbereiche zu verbessern, um sicherzustellen, dass die Sicherheitsprozesse angemessen auf Sicherheitsvorfälle und Notfallsituationen reagieren können.

Geschäftsprozesse

GP01 Konstruktion

Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	

GP02 Einkauf

Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	

GP03 Auftragsannahme / Verkauf

Beschreibung:	
---------------	--

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

GP04

Fertigung

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

GP05

Technischer Support

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

Anwendungen

A01

APP.1.1

Excel

Office-Produkte

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

APP.1.1.A2	Einschränken von Aktiven Inhalten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Anforderung wird durch GPO Richtlinie umgesetzt.
APP.1.1.A3	Sicheres Öffnen von Dokumenten aus externen Quellen [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Dokumente aus externen Quellen werden nicht auf Schadsoftware überprüft.
APP.1.1.A6	Testen neuer Versionen von Office-Produkten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Neue Versionen von Office-Produkten werden nicht vom Einsatz getestet.
APP.1.1.A10	Regelung der Software-Entwicklung durch Endbenutzer
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Entbehrlich
Umsetzungserläuterung:	Die Erfüllung der Anforderung ist nicht relevant, da es keine spezifischen Maßnahmen oder Regelungen bezüglich der Software-Entwicklung durch Endbenutzer gibt.
APP.1.1.A11	Geregelter Einsatz von Erweiterungen für Office-Produkte
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	
APP.1.1.A12	Verzicht auf Cloud-Speicherung [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Deaktiviert durch GPO Richtlinie.
APP.1.1.A13	Verwendung von Viewer-Funktionen [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Viewer-Funktionen werden nicht durch den Benutzer deaktiviert.

APP.1.1.A14	Schutz gegen nachträgliche Veränderungen von Dokumenten [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Diese Information wird in der schulung erwähnt aber nicht erprobt oder geprüft ob das durchgeführt wird.
APP.1.1.A17	Sensibilisierung zu spezifischen Office-Eigenschaften
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Wird im Rahmen der 30 Min. Schulung durchgeführt.
A02	Outlook
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	
A03	Delftship
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	
A04	TeamViewer
OPS.1.2.5	Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	

OPS.1.2.5.A1	Planung des Einsatzes der Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Planung der Fernwartung bezieht mindestens die Identifikation der fernwartungsfähigen IT-Systeme sowie die klare Festlegung der Verantwortlichkeiten für die Durchführung der Fernwartung mit ein.
OPS.1.2.5.A2	Sicherer Verbindlungsaufbau bei der Fernwartung von Clients [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Über die Fritzbox ist VPN eingerichtet.
OPS.1.2.5.A3	Absicherung der Schnittstellen zur Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Firewall Defender Firewalls auf allen Clients.
OPS.1.2.5.A5	Einsatz von Online-Diensten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	TeamViewer ist lokal installiert.
OPS.1.2.5.A6	Erstellung einer Richtlinie für die Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Keine Richtlinie zur Fernwartung wurde erstellt.
OPS.1.2.5.A7	Dokumentation bei der Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Die Dokumentation wird nur dann erstellt, wenn der server runtergefahren wird.

OPS.1.2.5.A8	Sichere Protokolle bei der Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Die Teamviewer Protokolle sind im Einsatz.
OPS.1.2.5.A9	Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Zur Beschaffung werden Fernwartungswerkzeuge eingesetzt, die auf dem Markt verfügbar sind.
OPS.1.2.5.A10	Umgang mit Fernwartungswerkzeugen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Nur Admin darf mit den Fernwartungswerkzeugen arbeiten.
OPS.1.2.5.A17	Authentisierungsmechanismen bei der Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Mehr-Faktor-Verfahren zur Authentisierung.
OPS.1.2.5.A19	Fernwartung durch Dritte
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Maßnahmen für diesen Fall.
OPS.1.2.5.A20	Betrieb der Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keinen Meldeprozess für Support- und Fernwartungsanliegen, nur per Anruf.
OPS.1.2.5.A21	Erstellung eines Notfallplans für den Ausfall der Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keinen Notfallplan für den Ausfall der Fernwartung.

OPS.1.2.5.A24	Absicherung integrierter Fernwartungssysteme
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Absicherung integrierter Fernwartungssysteme.
OPS.1.2.5.A25	Entkopplung der Kommunikation bei der Fernwartung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Kein Sprungserver wird dafür verwendet.
A05	Word
APP.1.1	Office-Produkte
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
APP.1.1.A2	Einschränken von Aktiven Inhalten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Anforderung wird durch GPO Richtlinie umgesetzt.
APP.1.1.A3	Sicheres Öffnen von Dokumenten aus externen Quellen [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Dokumente aus externen Quellen werden nicht auf Schadsoftware überprüft.
APP.1.1.A6	Testen neuer Versionen von Office-Produkten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Neue Versionen von Office-Produkten werden nicht vom Einsatz getestet.
APP.1.1.A10	Regelung der Software-Entwicklung durch Endbenutzende
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Entbehrlich
Umsetzungserläuterung:	Die Erfüllung der Anforderung ist nicht relevant, da es keine spezifischen Maßnahmen oder Regelungen bezüglich der Software-Entwicklung durch Endbenutzer gibt.

APP.1.1.A11	Geregelter Einsatz von Erweiterungen für Office-Produkte
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	
APP.1.1.A12	Verzicht auf Cloud-Speicherung [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Deaktiviert durch GPO Richtlinie.
APP.1.1.A13	Verwendung von Viewer-Funktionen [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Viewer-Funktionen werden nicht durch den Benutzer deaktiviert.
APP.1.1.A14	Schutz gegen nachträgliche Veränderungen von Dokumenten [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Diese Information wird in der Schulung erwähnt aber nicht erprobt oder geprüft ob das durchgeführt wird.
APP.1.1.A17	Sensibilisierung zu spezifischen Office-Eigenschaften
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Wird im Rahmen der 30 Min. Schulung durchgeführt.

IT-Systeme

AP1	WLAN Access Point Produktion
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

AP2

WLAN Access Point Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C1

Client Betrieb APC

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C1

Client Betrieb Laptop

SYS.3.1

Laptops

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Regelungen zur mobilen Nutzung von Laptops

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Teilweise

Umsetzungserläuterung:

Die Benutzenden werden auf die Regelungen zur mobilen Nutzung von Laptops innerhalb der 30 min Schulung hingewiesen.

SYS.3.1.A3	Einsatz von Personal Firewalls
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	MacBooks haben keine firewall, die firewall kann durch Benutzer manipuliert werden.
SYS.3.1.A6	Sicherheitsrichtlinien für Laptops
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Benutzenden werden hinsichtlich des Schutzbedarfs von Laptops und der dort gespeicherten Daten sensibilisiert.
SYS.3.1.A7	Geregelte Übergabe und Rücknahme eines Laptops [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
SYS.3.1.A8	Sicherer Anschluss von Laptops an Datennetze [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Dafür wird VPN Verbindung benutzt.
SYS.3.1.A9	Sicherer Fernzugriff mit Laptops
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Es wird ein VPN verwendet, um ins Firmennetz zu kommen.
SYS.3.1.A10	Abgleich der Datenbestände von Laptops [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Laptops werden nie platt gemacht und es werden keine Daten gelöscht.
SYS.3.1.A11	Sicherstellung der Energieversorgung von Laptops [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Ja, diese werden eingerichtet. Sollte das Gerät kein Strom bekommen, würde das ja auffallen.

SYS.3.1.A12	Verlustmeldung für Laptops [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Es wird gemeldet und protokolliert.
SYS.3.1.A13	Verschlüsselung von Laptops
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	MacOS - ja, Windows - nicht.
SYS.3.1.A14	Geeignete Aufbewahrung von Laptops [Benutzende]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Die Benutzer werden dazu angehalten, ob sie dies tun. Es wird aber nicht überprüft, daher ist keine klare ja oder nein Aussage möglich.
SYS.3.1.A15	Geeignete Auswahl von Laptops [Beschaffungsstelle]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Nein, die Laptops werden einfach gekauft.
C2	Client Produktion
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	
C3	Client Produktionsleiter
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C4

Client Sekretär

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C5

Client Geschäftsführung

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C6

Client CNC Fräse

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C7

Client Gussmaschine

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

D1

Drucker Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

D2

Drucker Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

HP1

Switch Betrieb

NET.3.1

Router und Switches

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

NET.3.1.A1

Sichere Grundkonfiguration eines Routers oder Switches

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Teilweise

Umsetzungserläuterung:

Es wird nur die Standardeinstellung verwendet. Diese ist bedingt sicher, nicht komplett schutzlos, sollte aber angepasst werden.

NET.3.1.A4	Schutz der Administrationsschnittstellen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Anforderung wurde nicht implementiert.
NET.3.1.A5	Schutz vor Fragmentierungsangriffen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Standardeinstellung bietet keinen richtigen Schutz.
NET.3.1.A6	Notfallzugriff auf Router und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Der Administrator hat einen direkten Zugriff auf die Switches und den Router.
NET.3.1.A7	Protokollierung bei Routern und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Geräte wurden so konfiguriert, dass folgende Ereignisse wie Systemfehler, Logdaten protokolliert werden.
NET.3.1.A8	Regelmäßige Datensicherung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Konfigurationsdateien von Routern und Switches werden regelmäßig gesichert.
NET.3.1.A9	Betriebsdokumentationen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Konfigurationsänderungen und sicherheitsrelevante Aufgaben werden nicht dokumentiert.
NET.3.1.A10	Erstellung einer Sicherheitsrichtlinie
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.

NET.3.1.A11	Beschaffung eines Routers oder Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A12	Erstellung einer Konfigurations-Checkliste für Router und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A13	Administration über ein gesondertes Managementnetz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A14	Schutz vor Missbrauch von ICMP-Nachrichten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A15	Bogon- und Spoofing-Filterung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Bogon- und Spoofing-Filterung wurde durch Standardeinstellung über Geräte-Konten implementiert.
NET.3.1.A16	Schutz vor „IPv6 Routing Header Type-0“-Angriffen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A17	Schutz vor DoS- und DDoS-Angriffen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.

NET.3.1.A18	Einrichtung von Access Control Lists
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A19	Sicherung von Switch-Ports
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Für die Clients - nein, für Server - ja.
NET.3.1.A20	Sicherheitsaspekte von Routing-Protokollen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Der Router authentisiert sich, wenn er Routing-Informationen austauscht oder Updates für Routing-Tabellen verschickt.
NET.3.1.A21	Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Der Router und Switches sind an ein zentrales Identitäts- und Berechtigungsmanagement angebunden.
NET.3.1.A22	Notfallvorsorge bei Routern und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A23	Revision und Penetrationstests
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
HP2	Switch Produktion
NET.3.1	Router und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	

NET.3.1.A1	Sichere Grundkonfiguration eines Routers oder Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Es wird nur die Standardeinstellung verwendet. Diese ist bedingt sicher, nicht komplett schutzlos, sollte aber angepasst werden.
NET.3.1.A4	Schutz der Administrationsschnittstellen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Anforderung wurde nicht implementiert.
NET.3.1.A5	Schutz vor Fragmentierungsangriffen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Standardeinstellung bietet keinen richtigen Schutz.
NET.3.1.A6	Notfallzugriff auf Router und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Der Administrator hat einen direkten Zugriff auf die Switches und den Router.
NET.3.1.A7	Protokollierung bei Routern und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Geräte wurden so konfiguriert, dass folgende Ereignisse wie Systemfehler, Logdaten protokolliert werden.
NET.3.1.A8	Regelmäßige Datensicherung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Konfigurationsdateien von Routern und Switches werden regelmäßig gesichert.

NET.3.1.A9	Betriebsdokumentationen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Konfigurationsänderungen und sicherheitsrelevante Aufgaben werden nicht dokumentiert.
NET.3.1.A10	Erstellung einer Sicherheitsrichtlinie
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A11	Beschaffung eines Routers oder Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A12	Erstellung einer Konfigurations-Checkliste für Router und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A13	Administration über ein gesondertes Managementnetz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A14	Schutz vor Missbrauch von ICMP-Nachrichten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A15	Bogon- und Spoofing-Filterung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Bogon- und Spoofing-Filterung wurde durch Standardeinstellung über Geräte-Konten implementiert.

NET.3.1.A16	Schutz vor „IPv6 Routing Header Type-0“-Angriffen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A17	Schutz vor DoS- und DDoS-Angriffen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A18	Einrichtung von Access Control Lists
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A19	Sicherung von Switch-Ports
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Für die Clients - nein, für Server - ja.
NET.3.1.A20	Sicherheitsaspekte von Routing-Protokollen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Der Router authentisiert sich, wenn er Routing-Informationen austauscht oder Updates für Routing-Tabellen verschickt.
NET.3.1.A21	Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Der Router und Switches sind an ein zentrales Identitäts- und Berechtigungsmanagement angebunden.
NET.3.1.A22	Notfallvorsorge bei Routern und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Nein

Umsetzungserläuterung:

Diese Anforderung wurde nicht umgesetzt.

N1 Firewall Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

N2 Firewall Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

R1 Router

NET.3.1

Router und Switches

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Sichere Grundkonfiguration eines Routers oder Switches

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Teilweise

Umsetzung bis:

Umsetzungsstatus:

Es wird nur die Standardeinstellung verwendet. Diese ist bedingt sicher, nicht komplett schutzlos, sollte aber angepasst werden.

NET.3.1.A4	Schutz der Administrationsschnittstellen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Anforderung wurde nicht implementiert.
NET.3.1.A5	Schutz vor Fragmentierungsangriffen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Standardeinstellung bietet keinen richtigen Schutz.
NET.3.1.A6	Notfallzugriff auf Router und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Der Administrator hat einen direkten Zugriff auf die Switches und den Router.
NET.3.1.A7	Protokollierung bei Routern und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Geräte wurden so konfiguriert, dass folgende Ereignisse wie Systemfehler, Logdaten protokolliert werden.
NET.3.1.A8	Regelmäßige Datensicherung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Konfigurationsdateien von Routern und Switches werden regelmäßig gesichert.
NET.3.1.A9	Betriebsdokumentationen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Konfigurationsänderungen und sicherheitsrelevante Aufgaben werden nicht dokumentiert.
NET.3.1.A10	Erstellung einer Sicherheitsrichtlinie
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.

NET.3.1.A11	Beschaffung eines Routers oder Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A12	Erstellung einer Konfigurations-Checkliste für Router und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A13	Administration über ein gesondertes Managementnetz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A14	Schutz vor Missbrauch von ICMP-Nachrichten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A15	Bogon- und Spoofing-Filterung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Bogon- und Spoofing-Filterung wurde durch Standardeinstellung über Geräte-Konten implementiert.
NET.3.1.A16	Schutz vor „IPv6 Routing Header Type-0“-Angriffen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A17	Schutz vor DoS- und DDoS-Angriffen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.

NET.3.1.A18	Einrichtung von Access Control Lists
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A19	Sicherung von Switch-Ports
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Für die Clients - nein, für Server - ja.
NET.3.1.A20	Sicherheitsaspekte von Routing-Protokollen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Der Router authentisiert sich, wenn er Routing-Informationen austauscht oder Updates für Routing-Tabellen verschickt.
NET.3.1.A21	Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Der Router und Switches sind an ein zentrales Identitäts- und Berechtigungsmanagement angebunden.
NET.3.1.A22	Notfallvorsorge bei Routern und Switches
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
NET.3.1.A23	Revision und Penetrationstests
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.

S1

SYS.1.1	Server Betrieb
	Allgemeiner Server

Beschreibung:

Hauptverantwortlicher:**Verantwortlicher:**

SYS.1.1.A1	Zugriffsschutz und Nutzung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Server stehen im Serverraum, durch kartensysteme geschützt, server steht im serverschrank, welcher mit einem schlüssel geschützt ist, schlüssel wird an assistenz weitergegeben wenn der chef nicht da ist. Der Systemadministrator und CEO haben den Schlüssel zum Serverraum.
SYS.1.1.A2	Authentisierung an Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Authentisierungsverfahren werden auf den Servern eingesetzt, die dem Schutzbedarf der Server angemessen sind.
SYS.1.1.A5	Schutz von Schnittstellen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Ja, durch die Sicherheitsmaßnahmen des gebäudes und des abgeschlossenen Serverschrankes.
SYS.1.1.A6	Deaktivierung nicht benötigter Dienste
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Der Server wird installiert und nur die benötigte software. Es werden also keine Änderungen an den Grundeinstellungen vorgenommen.
SYS.1.1.A9	Einsatz von Virenschutz-Programmen auf Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Standard Viren Programm wurde dafür eingesetzt.
SYS.1.1.A10	Protokollierung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Das System hat eine interne log datei, die alle sicherheitsrelevanten Systemereignisse mitschneidet. Es wird allerdings keine gesonderte Software verwendet.

SYS.1.1.A11	Festlegung einer Sicherheitsrichtlinie für Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Anforderungen an Server werden in einer separaten Sicherheitsrichtlinie nicht konkretisiert.
SYS.1.1.A12	Planung des Server-Einsatzes
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
SYS.1.1.A13	Beschaffung von Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
SYS.1.1.A15	Unterbrechungsfreie und stabile Stromversorgung [Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Eine USV ist angeschlossen.
SYS.1.1.A16	Sichere Installation und Grundkonfiguration von Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
SYS.1.1.A19	Einrichtung lokaler Paketfilter
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Einrichtung lokaler Paketfilter wurde teilweise umgesetzt.
SYS.1.1.A21	Betriebsdokumentation für Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Betriebsdokumentation.

SYS.1.1.A22	Einbindung in die Notfallplanung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keinen Notfallplan.
SYS.1.1.A23	Systemüberwachung und Monitoring von Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt kein Konzept für Systemüberwachung und Monitoring von Servern.
SYS.1.1.A24	Sicherheitsprüfungen für Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Server werden nicht gesondert geprüft.
SYS.1.1.A25	Geregelte Außerbetriebnahme eines Servers
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Wenn nötig, aber es gibt keinen Wartungsplan.
SYS.1.1.A35	Erstellung und Pflege eines Betriebshandbuchs
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt kein Betriebshandbuch.
SYS.1.1.A37	Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten.
SYS.1.1.A39	Zentrale Verwaltung der Sicherheitsrichtlinien von Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Zentrale Verwaltung der Sicherheitsrichtlinien von Servern.

SYS.1.2.3	Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
SYS.1.2.3.A1	Planung von Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Keine begründete und dokumentierte Entscheidung für eine geeignete Edition von Windows Server wird getroffen.
SYS.1.2.3.A2	Sichere Installation von Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt, es gibt nur Standard Variante.
SYS.1.2.3.A3	Telemetrie- und Nutzungsdaten unter Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
SYS.1.2.3.A4	Schutz vor Ausnutzung von Schwachstellen in Anwendungen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Standardkonfigurationen für den Exploit-Schutz wurden aktiviert.
SYS.1.2.3.A5	Sichere Authentisierung und Autorisierung in Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Nur Admin ist Motglied der Sicherheitsgruppe "Protected Users".
SYS.1.2.3.A6	Sicherheit beim Fernzugriff über RDP
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Gruppe der Berechtigten und IT-Systeme für den Remote-Desktopzugriff (RDP) wird durch die Zuweisung entsprechender Berechtigungen festgelegt.

SYS.1.1	Allgemeiner Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
SYS.1.1.A1	Zugriffsschutz und Nutzung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Server stehen im Serverraum, durch kartensysteme geschützt, server steht im serverschrank, welcher mit einem schlüssel geschützt ist, schlüssel wird an assistenz weitergegeben wenn der chef nicht da ist. Der Systemadministrator und CEO haben den Schlüssel zum Serverraum.
SYS.1.1.A2	Authentisierung an Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Authentisierungsverfahren werden auf den Servern eingesetzt, die dem Schutzbedarf der Server angemessen sind.
SYS.1.1.A5	Schutz von Schnittstellen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Ja, durch die Sicherheitsmaßnahmen des gebäudes und des abgeschlossenen Serverschrankes.
SYS.1.1.A6	Deaktivierung nicht benötigter Dienste
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Der Server wird installiert und nur die benötigte software. Es werden also keine Änderungen an den Grundeinstellungen vorgenommen.
SYS.1.1.A9	Einsatz von Virenschutz-Programmen auf Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Standard Viren Programm wurde dafür eingesetzt.

SYS.1.1.A10	Protokollierung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Das System hat eine interne log datei, die alle sicherheitsrelevanten Systemereignisse mitschneidet. Es wird allerdings keine gesonderte Software verwendet.
SYS.1.1.A11	Festlegung einer Sicherheitsrichtlinie für Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Die Anforderungen an Server werden in einer separaten Sicherheitsrichtlinie nicht konkretisiert.
SYS.1.1.A12	Planung des Server-Einsatzes
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
SYS.1.1.A13	Beschaffung von Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
SYS.1.1.A15	Unterbrechungsfreie und stabile Stromversorgung [Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Eine USV ist angeschlossen.
SYS.1.1.A16	Sichere Installation und Grundkonfiguration von Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
SYS.1.1.A19	Einrichtung lokaler Paketfilter
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Einrichtung lokaler Paketfilter wurde teilweise umgesetzt.

SYS.1.1.A21	Betriebsdokumentation für Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Betriebsdokumentation.
SYS.1.1.A22	Einbindung in die Notfallplanung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keinen Notfallplan.
SYS.1.1.A23	Systemüberwachung und Monitoring von Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt kein Konzept für Systemüberwachung und Monitoring von Servern.
SYS.1.1.A24	Sicherheitsprüfungen für Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Server werden nicht gesondert geprüft.
SYS.1.1.A25	Geregelte Außerbetriebnahme eines Servers
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Wenn nötig, aber es gibt keinen Wartungsplan.
SYS.1.1.A35	Erstellung und Pflege eines Betriebshandbuchs
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt kein Betriebshandbuch.
SYS.1.1.A37	Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten.

SYS.1.1.A39	Zentrale Verwaltung der Sicherheitsrichtlinien von Servern
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Es gibt keine Zentrale Verwaltung der Sicherheitsrichtlinien von Servern.
SYS.1.2.3	Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
SYS.1.2.3.A1	Planung von Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Keine begründete und dokumentierte Entscheidung für eine geeignete Edition von Windows Server wird getroffen.
SYS.1.2.3.A2	Sichere Installation von Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt, es gibt nur Standard Variante.
SYS.1.2.3.A3	Telemetrie- und Nutzungsdaten unter Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Nein
Umsetzungserläuterung:	Diese Anforderung wurde nicht umgesetzt.
SYS.1.2.3.A4	Schutz vor Ausnutzung von Schwachstellen in Anwendungen
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Standardkonfigurationen für den Exploit-Schutz wurden aktiviert.
SYS.1.2.3.A5	Sichere Authentisierung und Autorisierung in Windows Server
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Teilweise
Umsetzungserläuterung:	Nur Admin ist Mitglied der Sicherheitsgruppe "Protected Users".

SYS.1.2.3.A6	Sicherheit beim Fernzugriff über RDP
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Die Gruppe der Berechtigten und IT-Systeme für den Remote-Desktopzugriff (RDP) wird durch die Zuweisung entsprechender Berechtigungen festgelegt.

ICS-Systeme

S100	SPS
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	
S101	Produktionsmaschine - CNC Fräse
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	
S102	Produktionsmaschine - Gussmaschine
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	

Andere/IoT-Systeme

I1

Videoüberwachung

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

K1

Kaffeemaschine

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

Kommunikationsverbindungen

AP1↔N1

WLAN AP Betrieb↔Firewall Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

AP2↔N2

WLAN AP Produktion↔Firewall Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C1/4/5<AP2

Client Betrieb<WLAN AP Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C1/4/5<N1

Client Betrieb<Firewall Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C1<C2

Client Betrieb<Client Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C1<C4

Client Betrieb<Client Sekretär

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C1<C5

Client Betrieb<>Client Geschäftsführung

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C1<D1

Client Betrieb<>Drucker Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C1<S1

Client Betrieb<>Server Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C2/3/6/7<>AP1

Client Produktion<>WLAN AP Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C2/3↔S100/S101/102 Client Produktion/Produktionsleiter↔ICS-Systeme

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C2/C3/C6/C7↔N2 Client Produktion↔Firewall Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C2↔C3 Client Produktion↔Client Produktionsleiter

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C2<>C6**Client Produktion<>Client CNC Fräse**

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C2<>C7**Client Produktion<>Client Gussmaschine**

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C2<>D2**Client Produktion<>Drucker Produktion**

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C2<>S2**Client Produktion<>Server Produktion**

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C3<>D2**Client Produktionsleiter<>Drucker Produktion**

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C4<>C5**Client Sekretär<>Client Geschäftsführung**

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C4<>D1**Client Sekräter<>Drucker Betrieb**

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

C5<>D1**Client Geschäftsführung<>Drucker Betrieb**

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

HP1<‐S1

Switch Betrieb‐Server Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

HP2‐AP1

Switch Produktion‐WLAN AP Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

HP2‐C2/3

Switch Produktion‐Client Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

HP2‐N2

Switch Betrieb‐Firewall Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

HP2<>>S2

Switch Produktion<>>Drucker Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

HP2<>>S2

Switch Produktion<>>Server Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

K40

Firewall Prod <>> Router

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

K42

Router<>>Videoüberwachung

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

K43

Router<>>Internet

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

K44

Kaffeemaschine <>> WLAN AP PROD

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

K45

Firewall Betrieb<->Router

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

S1<>N1

Server Betrieb<>Firewall Betrieb

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

S1<>S2

Server Betrieb<>Server Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

S2<>N2

Server Produktion<>Firewall Produktion

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus: Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

Räume

Halle und Materiallager

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

EG-1

INF.7

Büroraum Geschäftsleiter

Büroarbeitsplatz

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

INF.7.A1

Geeignete Auswahl und Nutzung eines Büorraumes [Vorgesetzte]

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Ja

Umsetzungserläuterung:

Nur Räume, die den festgelegten Sicherheits- und Funktionalitätsstandards entsprechen, werden als Büroräume genutzt.

INF.7.A2

Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Ja

Umsetzungserläuterung:

Zur Gewährleistung der Sicherheit der Räumlichkeiten und zur Verhinderung unbefugten Zugangs stellen alle Mitarbeitenden sicher, dass Fenster geschlossen und Türen abgeschlossen sind, wenn sich die Räume nicht in Gebrauch befinden oder sich niemand im Raum aufhält.

INF.7.A3

Fliegende Verkabelung

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Ja

Umsetzungserläuterung:

Diese Anforderung wurde umgesetzt und trägt nicht nur zu einem effizienten Betrieb bei, sondern minimiert auch potenzielle Stolperfallen oder Unannehmlichkeiten im Raum.

INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der ergonomischen Maßnahmen wurde sichergestellt, dass die Arbeitsplätze den besten Standards für Benutzerfreundlichkeit, Sicherheit und Komfort entsprechen.
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der Maßnahmen zur Arbeitsplatzorganisation wird allen Mitarbeitenden nachdrücklich empfohlen, ihren Arbeitsplatz aufgeräumt zu hinterlassen.
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der empfohlenen Maßnahmen werden alle Mitarbeitenden dazu angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht in Gebrauch sind.
EG-2	Büroraum Personal
INF.7	Büroarbeitsplatz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
INF.7.A1	Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Nur Räume, die den festgelegten Sicherheits- und Funktionalitätsstandards entsprechen, werden als Büoräume genutzt.
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Zur Gewährleistung der Sicherheit der Räumlichkeiten und zur Verhinderung unbefugten Zugangs stellen alle Mitarbeitenden sicher, dass Fenster geschlossen und Türen abgeschlossen sind, wenn sich die Räume nicht in Gebrauch befinden oder sich niemand im Raum aufhält.

INF.7.A3	Fliegende Verkabelung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Diese Anforderung wurde umgesetzt und trägt nicht nur zu einem effizienten Betrieb bei, sondern minimiert auch potenzielle Stolperfallen oder Unannehmlichkeiten im Raum.
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der ergonomischen Maßnahmen wurde sichergestellt, dass die Arbeitsplätze den besten Standards für Benutzerfreundlichkeit, Sicherheit und Komfort entsprechen.
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der Maßnahmen zur Arbeitsplatzorganisation wird allen Mitarbeitenden nachdrücklich empfohlen, ihren Arbeitsplatz aufgeräumt zu hinterlassen.
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der empfohlenen Maßnahmen werden alle Mitarbeitenden dazu angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht in Gebrauch sind.
EG-3	Büroraum Entwicklung
INF.7	Büroarbeitsplatz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Zur Gewährleistung der Sicherheit der Räumlichkeiten und zur Verhinderung unbefugten Zugangs stellen alle Mitarbeitenden sicher, dass Fenster geschlossen und Türen abgeschlossen sind, wenn sich die Räume nicht in Gebrauch befinden oder sich niemand im Raum aufhält.

INF.7.A3	Fliegende Verkabelung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Diese Anforderung wurde umgesetzt und trägt nicht nur zu einem effizienten Betrieb bei, sondern minimiert auch potenzielle Stolperfallen oder Unannehmlichkeiten im Raum.
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der ergonomischen Maßnahmen wurde sichergestellt, dass die Arbeitsplätze den besten Standards für Benutzerfreundlichkeit, Sicherheit und Komfort entsprechen.
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der Maßnahmen zur Arbeitsplatzorganisation wird allen Mitarbeitenden nachdrücklich empfohlen, ihren Arbeitsplatz aufgeräumt zu hinterlassen.
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der empfohlenen Maßnahmen werden alle Mitarbeitenden dazu angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht in Gebrauch sind.
EG-4	Büroraum Einkauf
INF.7	Büroarbeitsplatz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
INF.7.A1	Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Nur Räume, die den festgelegten Sicherheits- und Funktionalitätsstandards entsprechen, werden als Büoräume genutzt.

INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Zur Gewährleistung der Sicherheit der Räumlichkeiten und zur Verhinderung unbefugten Zugangs stellen alle Mitarbeitenden sicher, dass Fenster geschlossen und Türen abgeschlossen sind, wenn sich die Räume nicht in Gebrauch befinden oder sich niemand im Raum aufhält.
INF.7.A3	Fliegende Verkabelung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Diese Anforderung wurde umgesetzt und trägt nicht nur zu einem effizienten Betrieb bei, sondern minimiert auch potenzielle Stolperfallen oder Unannehmlichkeiten im Raum.
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der ergonomischen Maßnahmen wurde sichergestellt, dass die Arbeitsplätze den besten Standards für Benutzerfreundlichkeit, Sicherheit und Komfort entsprechen.
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der Maßnahmen zur Arbeitsplatzorganisation wird allen Mitarbeitenden nachdrücklich empfohlen, ihren Arbeitsplatz aufgeräumt zu hinterlassen.
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der empfohlenen Maßnahmen werden alle Mitarbeitenden dazu angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht in Gebrauch sind.

EG-5

Empfang/Wartebereich

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

EG-6

Küche

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.

Umsetzungserläuterung:

LG-1

Büroraum Produktion

INF.7

Büroarbeitsplatz

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

INF.7.A1

Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte]

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Ja
Nur Räume, die den festgelegten Sicherheits- und Funktionalitätsstandards entsprechen, werden als Büoräume genutzt.

INF.7.A2

Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Ja
Zur Gewährleistung der Sicherheit der Räumlichkeiten und zur Verhinderung unbefugten Zugangs stellen alle Mitarbeitenden sicher, dass Fenster geschlossen und Türen abgeschlossen sind, wenn sich die Räume nicht in Gebrauch befinden oder sich niemand im Raum aufhält.

INF.7.A3

Fliegende Verkabelung

Beschreibung:

Hauptverantwortlicher:

Verantwortlicher:

Umsetzung durch:

Umsetzung bis:

Umsetzungsstatus:

Ja
Diese Anforderung wurde umgesetzt und trägt nicht nur zu einem effizienten Betrieb bei, sondern minimiert auch potenzielle Stolperfälle oder Unannehmlichkeiten im Raum.

INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der ergonomischen Maßnahmen wurde sichergestellt, dass die Arbeitsplätze den besten Standards für Benutzerfreundlichkeit, Sicherheit und Komfort entsprechen.
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der Maßnahmen zur Arbeitsplatzorganisation wird allen Mitarbeitenden nachdrücklich empfohlen, ihren Arbeitsplatz aufgeräumt zu hinterlassen.
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der empfohlenen Maßnahmen werden alle Mitarbeitenden dazu angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht in Gebrauch sind.

LG-2	Küche
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	

OG-1	Büroraum Vertrieb
INF.7	Büroarbeitsplatz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
INF.7.A1	Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Nur Räume, die den festgelegten Sicherheits- und Funktionalitätsstandards entsprechen, werden als Büroräume genutzt.

INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Zur Gewährleistung der Sicherheit der Räumlichkeiten und zur Verhinderung unbefugten Zugangs stellen alle Mitarbeitenden sicher, dass Fenster geschlossen und Türen abgeschlossen sind, wenn sich die Räume nicht in Gebrauch befinden oder sich niemand im Raum aufhält.
INF.7.A3	Fliegende Verkabelung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Diese Anforderung wurde umgesetzt und trägt nicht nur zu einem effizienten Betrieb bei, sondern minimiert auch potenzielle Stolperfallen oder Unannehmlichkeiten im Raum.
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der ergonomischen Maßnahmen wurde sichergestellt, dass die Arbeitsplätze den besten Standards für Benutzerfreundlichkeit, Sicherheit und Komfort entsprechen.
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der Maßnahmen zur Arbeitsplatzorganisation wird allen Mitarbeitenden nachdrücklich empfohlen, ihren Arbeitsplatz aufgeräumt zu hinterlassen.
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der empfohlenen Maßnahmen werden alle Mitarbeitenden dazu angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht in Gebrauch sind.

OG-2	Büroraum IT Admin
INF.7	Büroarbeitsplatz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	

INF.7.A1	Geeignete Auswahl und Nutzung eines Büorraumes [Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Nur Räume, die den festgelegten Sicherheits- und Funktionalitätsstandards entsprechen, werden als Büoräume genutzt.
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Zur Gewährleistung der Sicherheit der Räumlichkeiten und zur Verhinderung unbefugten Zugangs stellen alle Mitarbeitenden sicher, dass Fenster geschlossen und Türen abgeschlossen sind, wenn sich die Räume nicht in Gebrauch befinden oder sich niemand im Raum aufhält.
INF.7.A3	Fliegende Verkabelung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Diese Anforderung wurde umgesetzt und trägt nicht nur zu einem effizienten Betrieb bei, sondern minimiert auch potenzielle Stolperfallen oder Unannehmlichkeiten im Raum.
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der ergonomischen Maßnahmen wurde sichergestellt, dass die Arbeitsplätze den besten Standards für Benutzerfreundlichkeit, Sicherheit und Komfort entsprechen.
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der Maßnahmen zur Arbeitsplatzorganisation wird allen Mitarbeitenden nachdrücklich empfohlen, ihren Arbeitsplatz aufgeräumt zu hinterlassen.
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der empfohlenen Maßnahmen werden alle Mitarbeitenden dazu angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht in Gebrauch sind.

INF.7	Büroarbeitsplatz
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
INF.7.A1	Geeignete Auswahl und Nutzung eines Büorraumes [Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Nur Räume, die den festgelegten Sicherheits- und Funktionalitätsstandards entsprechen, werden als Büoräume genutzt.
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Zur Gewährleistung der Sicherheit der Räumlichkeiten und zur Verhinderung unbefugten Zugangs stellen alle Mitarbeitenden sicher, dass Fenster geschlossen und Türen abgeschlossen sind, wenn sich die Räume nicht in Gebrauch befinden oder sich niemand im Raum aufhält.
INF.7.A3	Fliegende Verkabelung
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Diese Anforderung wurde umgesetzt und trägt nicht nur zu einem effizienten Betrieb bei, sondern minimiert auch potenzielle Stolperfallen oder Unannehmlichkeiten im Raum.
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der ergonomischen Maßnahmen wurde sichergestellt, dass die Arbeitsplätze den besten Standards für Benutzerfreundlichkeit, Sicherheit und Komfort entsprechen.
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der Maßnahmen zur Arbeitsplatzorganisation wird allen Mitarbeitenden nachdrücklich empfohlen, ihren Arbeitsplatz aufgeräumt zu hinterlassen.

INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Ja
Umsetzungserläuterung:	Durch die erfolgreiche Umsetzung der empfohlenen Maßnahmen werden alle Mitarbeitenden dazu angewiesen, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht in Gebrauch sind.
OG-4	Pausenraum
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	
OG-5	Serverraum
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Beschreibung:	
Hauptverantwortlicher:	
Verantwortlicher:	
Umsetzung durch:	Umsetzung bis:
Umsetzungsstatus:	Hinweis: Werte können nicht abgeleitet werden, da keine Maßnahmen verknüpft sind.
Umsetzungserläuterung:	

A.5 Risikoanalyse

Informationsverbund:	Informationsverbund
Abkürzung:	SWDS
Abkürzung:	35
Geltungsbereich:	Kompletter Standort der Werft
Datum:	23.01.2024, 22:16
Autor:	Gruppe 4
Autor:	0.1
Freigabe:	Sebastian Breu
Vorgehensweise der Absicherung:	STANDARD

Definition der Schutzbedarfskategorien

Stufe: Unkritisch

<i>Gesetze/Vorschriften/Verträge</i>	Verstöße gegen Vorschriften und Gesetze mit keinen oder nur minimalen Konsequenzen. Keine oder nur minimale Vertragsverletzungen mit maximal geringen Konventionalstrafen.
<i>Selbstbestimmungsrecht</i>	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen nicht beeinträchtigt werden kann.
<i>persönliche Unversehrtheit</i>	Eine Beeinträchtigung ist nicht möglich.
<i>Aufgabenerfüllung</i>	Die Beeinträchtigung ist tolerabel. Die maximal tolerierbare Ausfallzeit ist größer als 72 Stunden.
<i>Innen-/Außenwirkung</i>	Es ist keine oder nur minimale Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.
<i>Finanzielle Auswirkungen</i>	Es ist kein oder nur minimaler finanzieller Schaden zu erwarten.

Stufe: Normal

<i>Gesetze/Vorschriften/Verträge</i>	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.
<i>Selbstbestimmungsrecht</i>	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
<i>persönliche Unversehrtheit</i>	Eine Beeinträchtigung erscheint nicht möglich.
<i>Aufgabenerfüllung</i>	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
<i>Innen-/Außenwirkung</i>	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
<i>Finanzielle Auswirkungen</i>	Der finanzielle Schaden bleibt für die Institution tolerabel.

Stufe: Hoch

<i>Gesetze/Vorschriften/Verträge</i>	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. Vertragsverletzungen mit hohen Konventionalstrafen.
<i>Selbstbestimmungsrecht</i>	

	Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
<i>persönliche Unversehrtheit</i>	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
<i>Aufgabenerfüllung</i>	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
<i>Innen-/Außenwirkung</i>	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
<i>Finanzielle Auswirkungen</i>	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Stufe: Sehr Hoch

<i>Gesetze/Vorschriften/Verträge</i>	Fundamentaler Verstoß gegen Vorschriften und Gesetze. Vertragsverletzungen, deren Haftungsschäden ruinös sind.
<i>Selbstbestimmungsrecht</i>	Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
<i>persönliche Unversehrtheit</i>	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben.
<i>Aufgabenerfüllung</i>	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
<i>Innen-/Außenwirkung</i>	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
<i>Finanzielle Auswirkungen</i>	Der finanzielle Schaden ist für die Institution existenzbedrohend.

Auswirkungen

existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.

Eintrittshäufigkeit

sehr häufig	Ereignis tritt mehrmals im Monat ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.

Risikokategorien

sehr hoch		Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.
hoch		Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
mittel		Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
gering		Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.

Risikomatrix

	Häufigkeit			
	mittel	hoch	sehr hoch	sehr hoch
existenzbedrohend	mittel	hoch	sehr hoch	sehr hoch
	mittel	mittel	hoch	sehr hoch
beträchtlich	gering	gering	mittel	hoch
	gering	gering	gering	gering
begrenzt	selten	mittel	häufig	sehr häufig
	selten	mittel	häufig	sehr häufig
vernachlässigbar	selten	mittel	häufig	sehr häufig
	selten	mittel	häufig	sehr häufig

Informationsverbund

SWDS Informationsverbund

G 0.2	Ungünstige klimatische Bedingungen	Betrifft Vertraulichkeit: Nein	Betrifft Integrität: Ja	Betrifft Verfügbarkeit: Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: begrenzt	Risikokategorie: gering	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: begrenzt	Risikokategorie: gering	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Implementierung von Backup- und Redundanzlösungen, um sicherzustellen, dass kritische Daten und Systeme auch bei physischen Schäden an einem Standort verfügbar bleiben.		
G 0.11	Ausfall oder Störung von Dienstleistungsunternehmen	Betrifft Vertraulichkeit: Ja	Betrifft Integrität: Ja	Betrifft Verfügbarkeit: Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung von Monitoring-Tools, um die Leistung und Verfügbarkeit von Dienstleistern proaktiv zu überwachen.		
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkung: beträchtlich	Risikokategorie: mittel	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit: Ja	Betrifft Integrität: Nein	Betrifft Verfügbarkeit: Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Implementierung von Ende-zu-Ende-Verschlüsselung, um sicherzustellen, dass Informationen während der Übertragung geschützt sind.		
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	Betrifft Vertraulichkeit: Ja	Betrifft Integrität: Nein	Betrifft Verfügbarkeit: Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Schulung der Mitarbeiter im Umgang mit physischer Sicherheit, um das Risiko von Diebstählen zu minimieren.		
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkung: beträchtlich	Risikokategorie: mittel	

Informationsverbund

SWDS Informationsverbund

G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit: Ja	Betrifft Integrität: Ja	Betrifft Verfügbarkeit: Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: begrenzt	Risikokategorie: gering	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: begrenzt	Risikokategorie: gering	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Kontinuierliche Überprüfung der Sicherheitsmaßnahmen und Anpassung an neue Bedrohungen oder technologische Veränderungen.		
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit: Ja	Betrifft Integrität: Nein	Betrifft Verfügbarkeit: Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: gefährlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: gefährlich	Risikokategorie: mittel	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Implementierung strenger Zugriffskontrollen, um sicherzustellen, dass nur autorisierte Benutzer auf schützenswerte Informationen zugreifen können.		
G 0.27	Ressourcenmangel	Betrifft Vertraulichkeit: Nein	Betrifft Integrität: Nein	Betrifft Verfügbarkeit: Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: begrenzt	Risikokategorie: gering	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: begrenzt	Risikokategorie: gering	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Durchführung regelmäßiger Risikobewertungen, um die wichtigsten Sicherheitsrisiken zu identifizieren und Ressourcen dort zu konzentrieren, wo sie am dringendsten benötigt werden		
G 0.29	Verstoß gegen Gesetze oder Regelungen	Betrifft Vertraulichkeit: Ja	Betrifft Integrität: Ja	Betrifft Verfügbarkeit: Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: gefährlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: unbearbeitet	Auswirkungen: unbearbeitet	Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Bereitstellung von Schulungen und Schulungsprogrammen für Mitarbeiter, um das Bewusstsein für gesetzliche Anforderungen zu schärfen und sicherzustellen, dass sie mit den Compliance-Richtlinien vertraut sind.		
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet	
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit: Ja	Betrifft Integrität: Ja	Betrifft Verfügbarkeit: Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: gefährlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: unbearbeitet	Auswirkungen: unbearbeitet	Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Implementierung klarer Richtlinien und Verfahren für die sichere Nutzung und Administration von Geräten.		

Informationsverbund

SWDS Informationsverbund

G 0.36	Identitätsdiebstahl	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: unbearbeitet		Auswirkungen: unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion			Erläuterungen: Implementierung starker Authentifizierungsmechanismen.			
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.38	Missbrauch personenbezogener Daten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: unbearbeitet		Auswirkungen: unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikovermeidung			Erläuterungen: Regelmäßige Datenschutzprüfungen und Überwachung von Datenzugriffen.			
G 0.42	Social Engineering	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: unbearbeitet		Auswirkungen: unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikovermeidung			Erläuterungen: Einsatz von Technologien zur Erkennung von Phishing-Angriffen.			

Geschäftsprozesse

GP01 Konstruktion	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Hoch
Erläuterungen:	Durch diese Analyse können potenzielle Risiken und Bedrohungen im Kontext der Schiffskonstruktion.		
GP02 Einkauf	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Hoch
Erläuterungen:	Durch diese Analyse können potenzielle Risiken und Bedrohungen im Kontext des Einkaufs von Schiffsdetails identifiziert werden.		
GP03 Auftragsannahme / Verkauf	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Hoch
Erläuterungen:	Durch diese Analyse können potenzielle Risiken und Bedrohungen im Kontext des Prozesses der Auftragsannahme und des Verkaufs identifiziert werden.		
GP04 Fertigung	Vertraulichkeit: Sehr hoch	Integrität: Sehr hoch	Verfügbarkeit: Sehr hoch
Erläuterungen:	Durch diese Analyse können potenzielle Risiken und Bedrohungen im Kontext des Prozesses der Fertigung von Schiffen identifiziert werden.		
GP05 Technischer Support	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Hoch
Erläuterungen:	Durch diese Analyse können potenzielle Risiken und Bedrohungen im Kontext des technischen Supports für Schiffsbau und -reparatur identifiziert werden.		

Anwendungen

A01 Excel		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Normal	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit: Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten	Betrifft Integrität: Ja	Auswirkungen: beträchtlich	Betrifft Verfügbarkeit: Nein	Betrifft Verfügbarkeit: Nein
	Risiko ohne zusätzliche Maßnahmen:						Risikokategorie: mittel
	Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Sicherzustellen, dass Office Produkte immer auf dem neuesten Stand ist.				
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit: Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Betrifft Integrität: Ja	Auswirkungen: begrenzt	Betrifft Verfügbarkeit: Ja	Risikokategorie: gering
	Risiko ohne zusätzliche Maßnahmen:						Risikokategorie: gering
	Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Regelmäßig Sicherheitsupdates und Patches für alle eingesetzten Systeme und Softwareprodukte einspielen, um bekannte Sicherheitslücken zu schließen. Die Produkte sollten gemäß den Herstellerempfehlungen und Best Practices eingesetzt werden. Dies erfordert Schulungen und Schulungsmaterialien für die Mitarbeiter, um sicherzustellen, dass die Technologien ordnungsgemäß verwendet werden.				
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit: Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Betrifft Integrität: Ja	Auswirkungen: beträchtlich	Betrifft Verfügbarkeit: Nein	Risikokategorie: mittel
	Risiko ohne zusätzliche Maßnahmen:						Risikokategorie: mittel
	Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Schulungen für Mitarbeiter, um das Bewusstsein für sichere Fernwartungspraktiken zu schärfen. Einführung von strikten Zugriffskontrollen und Authentifizierungsmechanismen für Fernwartungszugänge. Durchführung regelmäßiger Audits, um mögliche Schwachstellen frühzeitig zu erkennen und zu beheben.				
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	Betrifft Vertraulichkeit: Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten	Betrifft Integrität: Ja	Auswirkungen: beträchtlich	Betrifft Verfügbarkeit: Ja	Risikokategorie: mittel
	Risiko ohne zusätzliche Maßnahmen:						Risikokategorie: mittel
	Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Integration von Sicherheitsanforderungen in Verträge mit Lieferanten, um die Sicherheit der gelieferten Office Produkte oder Informationen zu gewährleisten.				

Anwendungen

A01 Excel		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Normal	
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: gefährlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkung: gefährlich		Risikokategorie: hoch	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Sensibilisierung der Mitarbeiter für die Bedeutung von Datenintegrität und sichere Handhabung von Informationen. Einsatz von Firewalls und Intrusion Detection Systemen, um unbefugte Zugriffe zu erkennen und zu verhindern.					
G 0.25	Ausfall von Geräten oder Systemen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: gefährlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: gefährlich		Risikokategorie: mittel	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Einführung von redundanten Systemen und Backup-Mechanismen, um einen nahtlosen Betrieb sicherzustellen.					
G 0.26	Fehlfunktion von Geräten oder Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: gefährlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkung: gefährlich		Risikokategorie: mittel	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Etablierung einer effektiven Backup-Strategie, um im Falle eines Systemausfalls wichtige Daten wiederherstellen zu können.					
G 0.28	Software-Schwachstellen oder -Fehler	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: gefährlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: gefährlich		Risikokategorie: mittel	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Sicherstellen, dass alle Office-Produkte regelmäßig auf aktuelle Softwareversionen aktualisiert werden, um bekannte Schwachstellen zu beheben.					
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: begrenzt		Risikokategorie: gering	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: begrenzt		Risikokategorie: gering	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Kontinuierliche Schulungsprogramme, um Mitarbeiter über neue Technologien und Verfahren auf dem Laufenden zu halten. Einrichtung eines effizienten Support- und Hilfeleistungssystems, um Benutzern bei auftretenden Problemen sofortige Unterstützung zu bieten.					

Anwendungen

A01 Excel		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Normal	
G 0.39	Schadprogramme	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkung: beträchtlich		Risikokategorie: hoch	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung von zuverlässiger Antivirensoftware auf allen relevanten Systemen. Kontinuierliche Aktualisierung von Betriebssystemen, Anwendungen und Sicherheitssoftware, um bekannte Schwachstellen zu beheben.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: begrenzt		Risikokategorie: gering	
G 0.46	Integritätsverlust schützenswerter Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: beträchtlich		Risikokategorie: mittel	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Nutzung von Versionierungsfunktionen, um Änderungen an Dokumenten nachzuverfolgen und wiederherstellen zu können.					
A04 TeamViewer		Vertraulichkeit: Hoch		Integrität: Normal		Verfügbarkeit: Normal	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkung: beträchtlich		Risikokategorie: mittel	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Eine Zwei-Faktor-Authentifizierung für den Zugriff auf die Fernwartungstools muss implementiert werden. Sicherzustellen, dass TeamViewer immer auf dem neuesten Stand ist.					
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: begrenzt		Risikokategorie: gering	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: begrenzt		Risikokategorie: gering	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Regelmäßig Sicherheitsupdates und Patches für alle eingesetzten Systeme und Softwareprodukte einspielen, um bekannte Sicherheitslücken zu schließen. Die Produkte sollten gemäß den Herstellerempfehlungen und Best Practices eingesetzt werden. Dies erfordert Schulungen und Schulungsmaterialien für die Mitarbeiter, um sicherzustellen, dass die Technologien ordnungsgemäß verwendet werden.					

Anwendungen

A04 TeamViewer		Vertraulichkeit: Hoch		Integrität: Normal		Verfügbarkeit: Normal	
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: beträchtlich		Risikokategorie: mittel	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Schulungen für Mitarbeiter, um das Bewusstsein für sichere Fernwartungspraktiken zu schärfen. Einführung von strikten Zugriffskontrollen und Authentifizierungsmechanismen für Fernwartungszugänge. Durchführung regelmäßiger Audits, um mögliche Schwachstellen frühzeitig zu erkennen und zu beheben.					
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkung: beträchtlich		Risikokategorie: mittel	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Integration von Sicherheitsanforderungen in Verträge mit Lieferanten, um die Sicherheit der gelieferten Produkte oder Informationen zu gewährleisten.					
G 0.21	Manipulation von Hard- oder Software	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Implementierung von Mechanismen zur regelmäßigen Überprüfung der Integrität von Hard- und Softwarekomponenten. Beschränkung von Zugriffsrechten auf Systemebene, um unautorisierte Änderungen zu verhindern.					
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkung: beträchtlich		Risikokategorie: hoch	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Sensibilisierung der Mitarbeiter für die Bedeutung von Datenintegrität und sichere Handhabung von Informationen. Einsatz von Firewalls und Intrusion Detection Systemen, um unbefugte Zugriffe zu erkennen und zu verhindern.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: begrenzt		Risikokategorie: gering	

Anwendungen

A04 TeamViewer		Vertraulichkeit: Hoch		Integrität: Normal		Verfügbarkeit: Normal	
G 0.25	Ausfall von Geräten oder Systemen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit:	mittel	Auswirkungen:	beträchtlich	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit:	mittel	Auswirkung:	beträchtlich	Risikokategorie:	mittel
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Einführung von redundanten Systemen und Backup-Mechanismen, um einen nahtlosen Betrieb sicherzustellen, selbst wenn ein Gerät ausfällt.					
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit:	häufig	Auswirkungen:	beträchtlich	Risikokategorie:	hoch
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit:	häufig	Auswirkung:	beträchtlich	Risikokategorie:	hoch
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung robuster Zugriffskontrollmechanismen, um sicherzustellen, dass nur autorisierte Benutzer auf Systeme zugreifen können. Durchführung regelmäßiger Überprüfungen der Benutzerberechtigungen, um sicherzustellen, dass nur notwendige Rechte vergeben sind.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit:	mittel	Auswirkung: begrenzt	Risikokategorie:	gering	
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit:	mittel	Auswirkungen: begrenzt	Risikokategorie:	gering	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit:	mittel	Auswirkung: begrenzt	Risikokategorie:	gering	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Kontinuierliche Schulungsprogramme, um Mitarbeiter über neue Technologien und Verfahren auf dem Laufenden zu halten. Einrichtung eines effizienten Support- und Hilfeleistungssystems, um Benutzern bei auftretenden Problemen sofortige Unterstützung zu bieten.					
G 0.37	Abstreiten von Handlungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit:	selten	Auswirkungen:	beträchtlich	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Implementierung einer sicheren Protokollierung, die Manipulationen durch Verschlüsselung und Integritätsprüfungen verhindert.					

Anwendungen

A04 TeamViewer		Vertraulichkeit: Hoch		Integrität: Normal		Verfügbarkeit: Normal	
G 0.39	Schadprogramme	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: häufig		Auswirkung: beträchtlich		Risikokategorie: hoch	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung von zuverlässiger Antivirensoftware auf allen relevanten Systemen. Kontinuierliche Aktualisierung von Betriebssystemen, Anwendungen und Sicherheitssoftware, um bekannte Schwachstellen zu beheben.				
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: begrenzt		Risikokategorie: gering	
G 0.40	Verhinderung von Diensten (Denial of Service)	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: selten		Auswirkung: beträchtlich		Risikokategorie: mittel	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Erhöhung der Netzwerkkapazität, um die Auswirkungen von volumetrischen Angriffen zu minimieren.				
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkung: begrenzt		Risikokategorie: gering	
A05 Word		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Normal	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: selten		Auswirkung: beträchtlich		Risikokategorie: mittel	
	Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Sicherzustellen, dass Office Produkte immer auf dem neuesten Stand ist.				
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: begrenzt		Risikokategorie: gering	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkung: begrenzt		Risikokategorie: gering	
	Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Regelmäßig Sicherheitsupdates und Patches für alle eingesetzten Systeme und Softwareprodukte einspielen, um bekannte Sicherheitslücken zu schließen. Die Produkte sollten gemäß den Herstellerempfehlungen und Best Practices eingesetzt werden. Dies erfordert Schulungen und Schulungsmaterialien für die Mitarbeiter, um sicherzustellen, dass die Technologien ordnungsgemäß verwendet werden.				

Anwendungen

A05 Word		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Normal	
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: beträchtlich		Risikokategorie:	mittel
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Schulungen für Mitarbeiter, um das Bewusstsein für sichere Fernwartungspraktiken zu schärfen. Einführung von strikten Zugriffskontrollen und Authentifizierungsmechanismen für Fernwartungszugänge. Durchführung regelmäßiger Audits, um mögliche Schwachstellen frühzeitig zu erkennen und zu beheben.					
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkung: beträchtlich		Risikokategorie:	mittel
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Integration von Sicherheitsanforderungen in Verträge mit Lieferanten, um die Sicherheit der gelieferten Office Produkte oder Informationen zu gewährleisten.					
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie:	hoch
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkung: beträchtlich		Risikokategorie:	hoch
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Sensibilisierung der Mitarbeiter für die Bedeutung von Datenintegrität und sichere Handhabung von Informationen. Einsatz von Firewalls und Intrusion Detection Systemen, um unbefugte Zugriffe zu erkennen und zu verhindern.					
G 0.25	Ausfall von Geräten oder Systemen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkung: beträchtlich		Risikokategorie:	mittel
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Einführung von redundanten Systemen und Backup-Mechanismen, um einen nahtlosen Betrieb sicherzustellen.					
G 0.26	Fehlfunktion von Geräten oder Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkung: beträchtlich		Risikokategorie:	mittel
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Etablierung einer effektiven Backup-Strategie, um im Falle eines Systemausfalls wichtige Daten wiederherstellen zu können.					

Anwendungen

A05 Word		Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Normal
G 0.28	Software-Schwachstellen oder -Fehler	Betrifft Vertraulichkeit: Risiko ohne Maßnahmen: Eintrittshäufigkeit: mittel	Betrifft Integrität: Risiko ohne zusätzliche Maßnahmen: Eintrittshäufigkeit: mittel	Betrifft Verfügbarkeit: Risikobehandlungsoption: Risikovermeidung
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit: Risiko ohne Maßnahmen: Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Betrifft Verfügbarkeit: Risikokategorie: mittel
				Risikokategorie: mittel
		Betrifft Vertraulichkeit: Risiko ohne zusätzliche Maßnahmen: Eintrittshäufigkeit: mittel	Auswirkung: beträchtlich	Risikokategorie: mittel
				Erläuterungen: Sicherstellen, dass alle Office-Produkte regelmäßig auf aktuelle Softwareversionen aktualisiert werden, um bekannte Schwachstellen zu beheben.
G 0.39	Schadprogramme	Betrifft Vertraulichkeit: Risiko ohne Maßnahmen: Eintrittshäufigkeit: häufig	Betrifft Integrität: Risiko ohne zusätzliche Maßnahmen: Eintrittshäufigkeit: häufig	Betrifft Verfügbarkeit: Risikokategorie: gering
				Risikokategorie: gering
		Betrifft Vertraulichkeit: Risikobehandlungsoption: Risikoreduktion	Auswirkungen: beträchtlich	Erläuterungen: Kontinuierliche Schulungsprogramme, um Mitarbeiter über neue Technologien und Verfahren auf dem Laufenden zu halten. Einrichtung eines effizienten Support- und Hilfeleistungssystems, um Benutzern bei auftretenden Problemen sofortige Unterstützung zu bieten.
				Risikokategorie: hoch
G 0.46	Integritätsverlust schützenswerter Informationen	Betrifft Vertraulichkeit: Risiko ohne Maßnahmen: Eintrittshäufigkeit: mittel	Betrifft Integrität: Risiko ohne zusätzliche Maßnahmen: Eintrittshäufigkeit: mittel	Betrifft Verfügbarkeit: Risikokategorie: hoch
				Risikokategorie: hoch
		Betrifft Vertraulichkeit: Risikobehandlungsoption: Risikovermeidung	Auswirkungen: beträchtlich	Erläuterungen: Implementierung von zuverlässiger Antivirensoftware auf allen relevanten Systemen. Kontinuierliche Aktualisierung von Betriebssystemen, Anwendungen und Sicherheitssoftware, um bekannte Schwachstellen zu beheben.
				Risikokategorie: gering

IT-Systeme

C1 Client Betrieb Laptop	Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Normal	
G 0.4 Verschmutzung, Staub, Korrosion	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit:	häufig	Auswirkungen:	begrenzt	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die (Verwendung von Schutzhüllen und regelmäßige Reinigung der Laptops sowie den Einsatz von Staubschutzvorrichtungen) werden die Laptops vor Verschmutzung, Staub und Korrosion geschützt.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
G 0.14 Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit:	mittel	Auswirkungen:	beträchtlich	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Datenschutzmaßnahmen, Sensibilisierung der Mitarbeiter für Sicherheitsrisiken und Schulung zur Erkennung von Spionageversuchen.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
G 0.15 Abhören	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit:	mittel	Auswirkungen:	beträchtlich	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Zudem sollten Sicherheitsmaßnahmen wie Firewalls und Antivirensoftware implementiert werden, um die Angriffsfläche zu minimieren und unautorisierten Zugriff zu erschweren. Schulungen und Sensibilisierungsmaßnahmen für Mitarbeitende können ebenfalls dazu beitragen, das Risiko von Spionageangriffen zu reduzieren.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit:	mittel	Auswirkungen:	beträchtlich	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikotransfer	Erläuterungen: Die Implementierung von Sicherheitsmaßnahmen wie Verschlüsselung von Datenträgern und Authentifizierungssystemen kann das Risiko eines Diebstahls von Geräten oder Datenträgern verringern.				

IT-Systeme

C1 Client Betrieb Laptop	Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Normal	
G 0.18 Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter können dazu beitragen, das Bewusstsein für Sicherheitsanforderungen zu schärfen und Fehlplanungen zu reduzieren.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.19 Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Verschlüsselungstechnologien und regelmäßige Überprüfungen der Zugriffsberechtigungen können helfen.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.21 Manipulation von Hard- oder Software	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Aktualisierungen, Sicherheitspatches und die Implementierung von Sicherheitslösungen können helfen.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.22 Manipulation von Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Schulung und Sensibilisierung der Mitarbeiter bezüglich sicherer Informationspraktiken können helfen.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet

IT-Systeme

C1 Client Betrieb Laptop	Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Normal	
G 0.23 Unbefugtes Eindringen in IT-Systeme	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: ChatGPT Schwachstelle: Technische Schwachstellen Bedrohung: Unbefugtes Eindringen in IT-Systeme Eintrittshäufigkeit: mittel bis hoch Risikobehandlung: Risikoreduktion Erläuterung zur Risikobehandlung: Die Implementierung von Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection Systemen und regelmäßigen Sicherheitsprüfungen kann das Risiko unbefugten Eindringens in IT-Systeme reduzieren. Die regelmäßige Aktualisierung von Software und Betriebssystemen, die Anwendung von sicheren Authentifizierungsmethoden und die Überwachung von Netzwerkaktivitäten, Schulungen für Mitarbeiter zur Erkennung von Phishing-Angriffen und anderen Methoden des unbefugten Zugriffs können das Risiko minimieren.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.24 Zerstörung von Geräten oder Datenträgern	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikotransfer	Erläuterungen: Die Risiken im Zusammenhang mit der Zerstörung von Geräten oder Datenträgern können durch den Abschluss von Versicherungen abgedeckt werden, um die finanziellen Auswirkungen zu minimieren.				
G 0.27 Ressourcenmangel	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Überprüfungen der Ressourcenverfügbarkeit, Implementierung von Kapazitätsmanagement-Tools, Schulungen für Mitarbeiter zur effektiven Nutzung von Ressourcen können das Risiko minimieren.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

C1 Client Betrieb Laptop		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Normal	
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Schulungen und Schulungsprogramme für Benutzer und Administratoren müssen implementiert werden.				
G 0.43	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
	Einspielen von Nachrichten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie:	hoch
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.45	Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Die Risikovermeidung kann durch den Einsatz von zuverlässigen Firewalls, Antivirus-Software und sicherheitsbewussten E-Mail-Filtern erfolgen.				
	Datenverlust	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
C4 Client Sekretär	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Backups und eine zuverlässige Datenwiederherstellungsstrategie sind nötig.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
	C5 Client Geschäftsführung	Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
	HP1 Switch Betrieb	Vertraulichkeit: Sehr hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie:	mittel
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung redundanter Netzwerkinfrastruktur, Backups und Notfallpläne ist nötig.				
C4 Client Sekretär	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
	C5 Client Geschäftsführung	Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
HP1 Switch Betrieb	Vertraulichkeit: Sehr hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch		

IT-Systeme

HP1 Switch Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Verschlüsselungstechnologien, die Auswirkungen von Spionageaktivitäten zu minimieren ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.15	Abhören	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Überprüfung und Aktualisierung der Sicherheitsprotokolle ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine proaktive Planung und Anpassung des Netzwerks ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Einführung wirksamer Zugriffskontrollen, Schulungsprogramme zur Sensibilisierung der Mitarbeitenden bezüglich des Umgangs mit schützenswerten Daten und Überwachungsmechanismen ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

HP1 Switch Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Verschlüsselung und regelmäßige Sicherheitsaudits sind nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.23	Unbefugtes Eindringen in IT-Systeme	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Schulungen, Einsatz von Firewalls und Intrusion Detection Systeme sind nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.25	Ausfall von Geräten oder Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Wartung und Überprüfung der Geräte können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.26	Fehlfunktion von Geräten oder Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Wartung und Überprüfung der Geräte sind nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

HP1 Switch Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.27	Ressourcenmangel	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie:	mittel
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Effizientes Ressourcenmanagement und Budgetoptimierung können das Risiko minimieren.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine strenge Zugriffskontrolle und Schulungen des Personals sind nötig.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine strenge Zugriffskontrolle und Schulungen des Personals sind nötig.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.37	Abstreiten von Handlungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten		Auswirkungen: begrenzt		Risikokategorie:	gering
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Protokollierungs- und Überwachungsmechanismen kann das Risiko minimieren.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet

IT-Systeme

HP1 Switch Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.40	Verhinderung von Diensten (Denial of Service)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.43	Einspielen von Nachrichten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.45	Datenverlust	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.46	Integritätsverlust schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

HP2 Switch Produktion		Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch	
G 0.9	Ausfall oder Störung von Kommunikationsnetze	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung redundanter Netzwerkinfrastruktur, Backups und Notfallpläne ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Verschlüsselungstechnologien, die Auswirkungen von Spionageaktivitäten zu minimieren ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.15	Abhören	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Überprüfung und Aktualisierung der Sicherheitsprotokolle ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine proaktive Planung und Anpassung des Netzwerks ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

HP2	Switch Produktion	Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch	
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Einführung wirksamer Zugriffskontrollen, Schulungsprogramme zur Sensibilisierung der Mitarbeitenden bezüglich des Umgangs mit schützenswerten Daten und Überwachungsmechanismen ist nötig.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Verschlüsselung und regelmäßige Sicherheitsaudits sind nötig.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.23	Unbefugtes Eindringen in IT-Systeme	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Schulungen, Einsatz von Firewalls und Intrusion Detection Systeme sind nötig.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.25	Ausfall von Geräten oder Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Wartung und Überprüfung der Geräte können das Risiko minimieren.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

HP2	Switch Produktion	Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch	
G 0.26	Fehlfunktion von Geräten oder Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Wartung und Überprüfung der Geräte sind nötig.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.27	Ressourcenmangel	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Effizientes Ressourcenmanagement und Budgetoptimierung können das Risiko minimieren.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine strenge Zugriffskontrolle und Schulungen des Personals sind nötig.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine strenge Zugriffskontrolle und Schulungen des Personals sind nötig.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

HP2 Switch Produktion		Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch	
G 0.37	Abstreiten von Handlungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: begrenzt		Risikokategorie: gering	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Protokollierungs- und Überwachungsmechanismen kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.40	Verhinderung von Diensten (Denial of Service)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.43	Einspielen von Nachrichten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.45	Datenverlust	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

HP2 Switch Produktion		Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch	
G 0.46	Integritätsverlust schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
R1 Router		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.9	Ausfall oder Störung von Kommunikationsnetze	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung redundanter Netzwerkinfrastruktur, Backups und Notfallpläne ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Verschlüsselungstechnologien, die Auswirkungen von Spionageaktivitäten zu minimieren ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.15	Abhören	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Überprüfung und Aktualisierung der Sicherheitsprotokolle ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

R1 Router		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine proaktive Planung und Anpassung des Netzwerks ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Einführung wirksamer Zugriffskontrollen, Schulungsprogramme zur Sensibilisierung der Mitarbeitenden bezüglich des Umgangs mit schützenswerten Daten und Überwachungsmechanismen ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Verschlüsselung und regelmäßige Sicherheitsaudits sind nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.23	Unbefugtes Eindringen in IT-Systeme	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Schulungen, Einsatz von Firewalls und Intrusion Detection Systeme sind nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

R1 Router		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.25	Ausfall von Geräten oder Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Wartung und Überprüfung der Geräte können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.26	Fehlfunktion von Geräten oder Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Wartung und Überprüfung der Geräte sind nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.27	Ressourcenmangel	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Effizientes Ressourcenmanagement und Budgetoptimierung können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine strenge Zugriffskontrolle und Schulungen des Personals sind nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

R1 Router		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine strenge Zugriffskontrolle und Schulungen des Personals sind nötig.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.37	Abstreiten von Handlungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: begrenzt	Risikokategorie: gering				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Protokollierungs- und Überwachungsmechanismen kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.40	Verhinderung von Diensten (Denial of Service)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.43	Einspielen von Nachrichten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				

IT-Systeme

R1 Router		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.45	Datenverlust	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.46	Integritätsverlust schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Mechanismen zur Authentifizierung, Autorisierung, regelmäßige Schulungen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
S1 Server Betrieb	Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch		
G 0.8	Ausfall oder Störung der Stromversorgung	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Der Einsatz von USV-Geräten, Backup-Stromquellen und regelmäßige Wartung der Strominfrastruktur können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Einführung von Sicherheitsrichtlinien, Zugriffskontrollen, Verschlüsselung und Überwachung können das Risiko reduzieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

S1 Server Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: selten	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Einführung von physischen Zugangskontrollen, Überwachungssystemen und der Verschlüsselung von Daten auf Datenträgern kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine kontinuierliche Überprüfung und Anpassung der IT-Infrastruktur sowie die Implementierung von Change-Management-Prozessen kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig	Auswirkungen: beträchtlich	Risikokategorie: hoch				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Einführung von strikten Zugriffskontrollen, Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Einführung von Überprüfungsprozessen, um sicherzustellen, dass Informationen und Produkte aus vertrauenswürdigen Quellen stammen ist nötig.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				

IT-Systeme

S1 Server Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.21	Manipulation von Hard- oder Software	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Sicherheitsmaßnahmen wie Verschlüsselung, regelmäßige Überprüfungen der Integrität von Hard- und Software sowie die zeitnahe Aktualisierung von Sicherheitspatches können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Zugriffskontrollen und die Verschlüsselung sensibler Informationen kann das Risiko minimiert werden.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.23	Unbefugtes Eindringen in IT-Systeme	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Schulungen für die Mitarbeiter können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.25	Ausfall von Geräten oder Systemen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Wartung und Überwachung, ein Notfallwiederherstellungsplan können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet

IT-Systeme

S1 Server Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.26	Fehlfunktion von Geräten oder Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Wartung und Qualitätskontrolle von Geräten können das Risiko minimieren.				
G 0.27	Ressourcenmangel	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: begrenzt		Risikokategorie: gering	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine effiziente Ressourcenplanung, klare Priorisierung von kritischen Systemen und regelmäßige Überwachung des Budgets können das Risiko minimieren.				
G 0.28	Software-Schwachstellen oder -Fehler	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Aktualisierung und Patching der Software können das Risiko minimieren.				
G 0.29	Verstoß gegen Gesetze oder Regelungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung eines Compliance-Management-Systems kann das Risiko minimieren.				
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

S1 Server Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig	Auswirkungen: beträchtlich	Risikokategorie: hoch				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Zugriffskontrollen und starken Authentifizierungsmethoden kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig	Auswirkungen: beträchtlich	Risikokategorie: hoch				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Schulung und Sensibilisierung der Mitarbeiter für korrekte Nutzung und Administration, Implementierung von Sicherheitsrichtlinien können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.32	Missbrauch von Berechtigungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Überprüfung und Anpassung von Berechtigungen ist nötig.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.37	Abstreiten von Handlungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Protokollierungssystemen, sowie Schulung der Mitarbeiter können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				

IT-Systeme

S1 Server Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.39	Schadprogramme	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Ein Einsatz von Antiviren- und Anti-Malware-Programmen, regelmäßige Aktualisierung von Software und Systemen, Sensibilisierung der Benutzer können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.40	Verhinderung von Diensten (Denial of Service)	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Sicherheitsmechanismen und Intrusion Prevention Systems, Überwachung der Netzwerke können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.43	Einspielen von Nachrichten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Verschlüsselung von Nachrichten, Implementierung von Authentifizierungsmechanismen, Schulungen für Benutzer zur Sensibilisierung für Sicherheitsrisiken können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.45	Datenverlust	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Datensicherungen, Implementierung von Redundanzmechanismen, Schulungen für Benutzer können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

S1 Server Betrieb		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Sehr hoch	
G 0.46	Integritätsverlust schützenswerter Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Zugriffskontrollen, Verschlüsselung von sensiblen Informationen und Überwachung der Datenintegrität können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
S2 Server Produktion		Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch	
G 0.8	Ausfall oder Störung der Stromversorgung	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Der Einsatz von USV-Geräten, Backup-Stromquellen und regelmäßige Wartung der Strominfrastruktur können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Einführung von Sicherheitsrichtlinien, Zugriffskontrollen, Verschlüsselung und Überwachung können das Risiko reduzieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Einführung von physischen Zugangskontrollen, Überwachungssystemen und der Verschlüsselung von Daten auf Datenträgern kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

S2 Server Produktion	Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch		
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine kontinuierliche Überprüfung und Anpassung der IT-Infrastruktur sowie die Implementierung von Change-Management-Prozessen kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Einführung von strikten Zugriffskontrollen, Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Einführung von Überprüfungsprozessen, um sicherzustellen, dass Informationen und Produkte aus vertrauenswürdigen Quellen stammen ist nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.21	Manipulation von Hard- oder Software	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Sicherheitsmaßnahmen wie Verschlüsselung, regelmäßige Überprüfungen der Integrität von Hard- und Software sowie die zeitnahe Aktualisierung von Sicherheitspatches können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

S2 Server Produktion		Vertraulichkeit: Sehr hoch	Integrität: Sehr hoch	Verfügbarkeit: Sehr hoch
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit: Nein	Betrifft Integrität: Ja	Betrifft Verfügbarkeit: Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Zugriffskontrollen und die Verschlüsselung sensibler Informationen kann das Risiko minimiert werden.		
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet	
G 0.23	Unbefugtes Eindringen in IT-Systeme	Betrifft Vertraulichkeit: Ja	Betrifft Integrität: Ja	Betrifft Verfügbarkeit: Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Schulungen für die Mitarbeiter können das Risiko minimieren.		
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet	
G 0.25	Ausfall von Geräten oder Systemen	Betrifft Vertraulichkeit: Nein	Betrifft Integrität: Nein	Betrifft Verfügbarkeit: Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Wartung und Überwachung, ein Notfallwiederherstellungsplan können das Risiko minimieren.		
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet	
G 0.26	Fehlfunktion von Geräten oder Systemen	Betrifft Vertraulichkeit: Ja	Betrifft Integrität: Ja	Betrifft Verfügbarkeit: Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Wartung und Qualitätskontrolle von Geräten können das Risiko minimieren.		
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet	

IT-Systeme

S2 Server Produktion		Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch	
G 0.27	Ressourcenmangel	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: begrenzt		Risikokategorie: gering	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Eine effiziente Ressourcenplanung, klare Priorisierung von kritischen Systemen und regelmäßige Überwachung des Budgets können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.28	Software-Schwachstellen oder -Fehler	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Aktualisierung und Patching der Software können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.29	Verstoß gegen Gesetze oder Regelungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung eines Compliance-Management-Systems kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Durch die Implementierung von Zugriffskontrollen und starken Authentifizierungsmethoden kann das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

S2 Server Produktion	Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch	
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Schulung und Sensibilisierung der Mitarbeiter für korrekte Nutzung und Administration, Implementierung von Sicherheitsrichtlinien können das Risiko minimieren.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.32 Missbrauch von Berechtigungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die regelmäßige Überprüfung und Anpassung von Berechtigungen ist nötig.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.37 Abstreiten von Handlungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Protokollierungssystemen, sowie Schulung der Mitarbeiter können das Risiko minimieren.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.39 Schadprogramme	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig		Auswirkungen: beträchtlich		Risikokategorie: hoch	
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Ein Einsatz von Antiviren- und Anti-Malware-Programmen, regelmäßige Aktualisierung von Software und Systemen, Sensibilisierung der Benutzer können das Risiko minimieren.				
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

IT-Systeme

S2 Server Produktion		Vertraulichkeit: Sehr hoch		Integrität: Sehr hoch		Verfügbarkeit: Sehr hoch	
G 0.40	Verhinderung von Diensten (Denial of Service)	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Sicherheitsmechanismen und Intrusion Prevention Systems, Überwachung der Netzwerke können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.43	Einspielen von Nachrichten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig	Auswirkungen: beträchtlich	Risikokategorie: hoch				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Verschlüsselung von Nachrichten, Implementierung von Authentifizierungsmechanismen, Schulungen für Benutzer zur Sensibilisierung für Sicherheitsrisiken können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.45	Datenverlust	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Regelmäßige Datensicherungen, Implementierung von Redundanzmechanismen, Schulungen für Benutzer können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.46	Integritätsverlust schützenswerter Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Zugriffskontrollen, Verschlüsselung von sensiblen Informationen und Überwachung der Datenintegrität können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				

Kommunikationsverbindungen

C1/4/5<>AP2 Client Betrieb<>WLAN AP Betrieb	Vertraulichkeit: Normal	Integrität: Hoch	Verfügbarkeit: Hoch
C1<>C2 Client Betrieb<>Client Produktion	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Normal
C1<>C4 Client Betrieb<>Client Sekretär	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Normal
C1<>C5 Client Betrieb<>Client Geschäftsführung	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Hoch
C1<>S1 Client Betrieb<>Server Betrieb	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Hoch
C2<>S2 Client Produktion<>Server Produktion	Vertraulichkeit: Sehr hoch	Integrität: Sehr hoch	Verfügbarkeit: Sehr hoch
HP1<>AP2 Switch Betrieb<>WLAN AP Betrieb	Vertraulichkeit: Normal	Integrität: Hoch	Verfügbarkeit: Hoch
HP1<>C1/4/5 Switch Betrieb<>Client Betrieb	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Sehr hoch
HP1<>D1 Switch Betrieb<>Drucker Betrieb	Vertraulichkeit: Normal	Integrität: Normal	Verfügbarkeit: Hoch
HP1<>N1 Server Betrieb<>Firewall Betrieb	Vertraulichkeit: Sehr hoch	Integrität: Sehr hoch	Verfügbarkeit: Sehr hoch
HP1<>S1 Switch Betrieb<>Server Betrieb	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Sehr hoch
HP2<->AP1 Switch Produktion<>WLAN AP Produktion	Vertraulichkeit: Normal	Integrität: Hoch	Verfügbarkeit: Hoch
HP2<>C2/3 Switch Produktion<>Client Produktion	Vertraulichkeit: Sehr hoch	Integrität: Sehr hoch	Verfügbarkeit: Sehr hoch
HP2<>N2 Switch Betrieb<>Firewall Betrieb	Vertraulichkeit: Sehr hoch	Integrität: Sehr hoch	Verfügbarkeit: Sehr hoch
HP2<>S2 Switch Produktion<>Drucker Produktion	Vertraulichkeit: Normal	Integrität: Normal	Verfügbarkeit: Hoch
HP2<>S2 Switch Produktion<>Server Produktion	Vertraulichkeit: Sehr hoch	Integrität: Sehr hoch	Verfügbarkeit: Sehr hoch
K40 Firewall Prod <> Router K42	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Sehr hoch
Router<>Videoüberwachung	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Normal
K43 Router<>Internet	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Sehr hoch
K45 Firewall Betrieb<->Router	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Hoch
S1<>N1 Server Betrieb<>Firewall Betrieb	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Unbearbeitet
S1<>S2 Server Betrieb<>Server Produktion	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Hoch
S2<>N2 Server Produktion<>Firewall Produktion	Vertraulichkeit: Hoch	Integrität: Hoch	Verfügbarkeit: Hoch

Räume

EG-1 Büroraum Geschäftsleiter		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.1	Feuer	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Die Implementierung angemessener Brandschutzmaßnahmen, Schulung von Mitarbeitenden für den Umgang mit Feuergefahren, Einsatz von Feuermeldern und Löschvorrichtungen können das Risiko minimieren.					
G 0.1	Feuer	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Die Implementierung angemessener Brandschutzmaßnahmen, Schulung von Mitarbeitenden für den Umgang mit Feuergefahren, Einsatz von Feuermeldern und Löschvorrichtungen können das Risiko minimieren.					
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Zugangskontrollen, Nutzung von Sicherheitssoftware können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Die Implementierung von Diebstahlschutzmaßnahmen wie Sicherheitskabeln, Diebstahlwarnsystemen, und regelmäßigen Schulungen für Mitarbeiter sind nötig, um dieses Risiko zu vermeiden.					

Räume

EG-1 Büroraum Geschäftsführer		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Die Implementierung von Diebstahlschutzmaßnahmen wie Sicherheitskabeln, Diebstahlwarnsystemen, und regelmäßigen Schulungen für Mitarbeiter sind nötig, um dieses Risiko zu vermeiden.					
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung effizienter Planungs- und Anpassungsprozesse, regelmäßige Überprüfung und Anpassung von Geschäftsabläufen können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung effizienter Planungs- und Anpassungsprozesse, regelmäßige Überprüfung und Anpassung von Geschäftsabläufen können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoakzeptanz	Erläuterungen: Schulungen für Mitarbeiter sind nötig.					
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoakzeptanz	Erläuterungen: Schulungen für Mitarbeiter sind nötig.					

Räume

EG-1 Büroraum Geschäftsleiter		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit:	mittel	Auswirkungen:	beträchtlich	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung von Zugangskontrollen, Nutzung von Sicherheitssoftware, regelmäßige Schulungen für Mitarbeiter können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit:	mittel	Auswirkungen:	beträchtlich	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung von Zugangskontrollen, Nutzung von Sicherheitssoftware, regelmäßige Schulungen für Mitarbeiter können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
G 0.29	Verstoß gegen Gesetze oder Regelungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit:	mittel	Auswirkungen:	beträchtlich	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung eines effektiven Compliance-Management-Systems, regelmäßige Schulungen für Mitarbeiter können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
G 0.29	Verstoß gegen Gesetze oder Regelungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit:	mittel	Auswirkungen:	beträchtlich	Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung eines effektiven Compliance-Management-Systems, regelmäßige Schulungen für Mitarbeiter können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit:	Unbearbeitet	Auswirkung:	Unbearbeitet	Risikokategorie:	unbearbeitet

Räume

EG-1 Büroraum Geschäftsleiter		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig	Auswirkungen: unbearbeitet	Risikokategorie: unbearbeitet				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung strenger Zugriffskontrollen, regelmäßige Sicherheitsüberprüfungen, Schulungen sind nötig.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: häufig	Auswirkungen: unbearbeitet	Risikokategorie: unbearbeitet				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung strenger Zugriffskontrollen, regelmäßige Sicherheitsüberprüfungen, Schulungen sind nötig.					
Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
G 0.33	Personalausfall	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Implementierung von klaren Vertretungsregelungen, Dokumentation von Arbeitsprozessen und Schulung von Vertretungspersonen sind nötig, um das Risiko zu minimieren.					
G 0.33	Personalausfall	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel	Auswirkungen: beträchtlich	Risikokategorie: mittel				
Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet	Auswirkung: Unbearbeitet	Risikokategorie: unbearbeitet				
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Implementierung von klaren Vertretungsregelungen, Dokumentation von Arbeitsprozessen und Schulung von Vertretungspersonen sind nötig, um das Risiko zu minimieren.					

Räume

EG-1 Büroraum Geschäftsführer		Vertraulichkeit: Hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung verbesserter Sicherheitsmaßnahmen wie Zugangskontrollen, Überwachungskameras und Sicherheitspersonal können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung verbesserter Sicherheitsmaßnahmen wie Zugangskontrollen, Überwachungskameras und Sicherheitspersonal können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
EG-2 Büroraum Personal		Vertraulichkeit: Sehr hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.1	Feuer	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: selten		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Die Implementierung angemessener Brandschutzmaßnahmen, Schulung von Mitarbeitenden für den Umgang mit Feuergefahren, Einsatz von Feuermeldern und Löschvorrichtungen können das Risiko minimieren.					
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Die Implementierung von Zugangskontrollen, Nutzung von Sicherheitssoftware können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

Räume

EG-2 Büroraum Personal		Vertraulichkeit: Sehr hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.14	Ausspähen von Informationen (Spionage)	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Nein
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: selten		Auswirkung: beträchtlich		Risikokategorie: mittel	
	Risikobehandlungsoption:	Risikoreduktion		Erläuterungen: Die Implementierung von Zugangskontrollen, Nutzung von Sicherheitssoftware können das Risiko minimieren.			
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikovermeidung		Erläuterungen: Die Implementierung von Diebstahlschutzmaßnahmen wie Sicherheitskabeln, Diebstahlwarnsystemen, und regelmäßigen Schulungen für Mitarbeiter sind nötig, um dieses Risiko zu vermeiden.			
G 0.18	Fehlplanung oder fehlende Anpassung	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoreduktion		Erläuterungen: Implementierung effizienter Planungs- und Anpassungsprozesse, regelmäßige Überprüfung und Anpassung von Geschäftsabläufen können das Risiko minimieren.			
	Risiko mit zusätzlichen Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
G 0.19	Offenlegung schützenswerter Informationen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
	Risiko ohne zusätzliche Maßnahmen:	Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
	Risikobehandlungsoption:	Risikoakzeptanz		Erläuterungen: Schulungen für Mitarbeiter sind nötig.			

Räume

EG-2 Büroraum Personal		Vertraulichkeit: Sehr hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.22	Manipulation von Informationen	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung von Zugangskontrollen, Nutzung von Sicherheitssoftware, regelmäßige Schulungen für Mitarbeiter können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.29	Verstoß gegen Gesetze oder Regelungen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung eines effektiven Compliance-Management-Systems, regelmäßige Schulungen für Mitarbeiter können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: häufig		Auswirkungen: unbearbeitet		Risikokategorie:	unbearbeitet
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung strenger Zugriffskontrollen, regelmäßige Sicherheitsüberprüfungen, Schulungen sind nötig.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
G 0.33	Personalausfall	Betrifft Vertraulichkeit:	Nein	Betrifft Integrität:	Nein	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie:	mittel
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie:	unbearbeitet
Risikobehandlungsoption:	Risikovermeidung	Erläuterungen: Implementierung von klaren Vertretungsregelungen, Dokumentation von Arbeitsprozessen und Schulung von Vertretungspersonen sind nötig, um das Risiko zu minimieren.					

Räume

EG-2 Büroraum Personal		Vertraulichkeit: Sehr hoch		Integrität: Hoch		Verfügbarkeit: Hoch	
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	Betrifft Vertraulichkeit:	Ja	Betrifft Integrität:	Ja	Betrifft Verfügbarkeit:	Ja
Risiko ohne Maßnahmen:		Eintrittshäufigkeit: mittel		Auswirkungen: beträchtlich		Risikokategorie: mittel	
Risiko ohne zusätzliche Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	
Risikobehandlungsoption:	Risikoreduktion	Erläuterungen: Implementierung verbesserter Sicherheitsmaßnahmen wie Zugangskontrollen, Überwachungskameras und Sicherheitspersonal können das Risiko minimieren.					
Risiko mit zusätzlichen Maßnahmen:		Eintrittshäufigkeit: Unbearbeitet		Auswirkung: Unbearbeitet		Risikokategorie: unbearbeitet	

BSI IT-Grundschutz: A.6 Realisierungsplan

Informationsverbund:	Informationsverbund
Abkürzung:	SWDS
Mitarbeiter:	35
Geltungsbereich:	Kompletter Standort der Werft
Datum:	23.01.2024, 22:17
Autor:	Gruppe 4
Version:	0.1
Freigabe:	Sebastian Breu
Vorgehensweise der Absicherung:	STANDARD

Informationsverbund

ORP.3	Sensibilisierung und Schulung zur Informationssicherheit			R1
SWDS	Informationsverbund			
	Kompletter Standort der Werft			
ORP.3.A1	Sensibilisierung der Institutionsleitung für Informationssicherheit [Vorgesetzte, Institutionsleitung]			
	Umsetzungstatus: Teilweise	Umsetzung bis: 20.6.2024	Umsetzung durch:	
	Erläuterung:	30 minuten schulung ist nicht genug - der inhalt ist auch allgemein und nicht spezifiziert.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
ORP.3.A3	Einweisung des Personals in den sicheren Umgang mit IT [Vorgesetzte, Personalabteilung, IT-Betrieb]			
	Umsetzungstatus: Teilweise	Umsetzung bis: 10.4.2024	Umsetzung durch:	
	Erläuterung:	30 minuten schulung ist nicht genug - der inhalt ist auch allgemein und nicht spezifiziert.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:

ORP.3	Sensibilisierung und Schulung zur Informationssicherheit			R1
SWDS	Informationsverbund			
	Kompletter Standort der Werft			
ORP.3.A4	Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit			
	Umsetzungstatus: Nein	Umsetzung bis: 27.3.2024	Umsetzung durch:	
	Erläuterung:	Es gibt eine schulung von 30 minuten welche aber keinem klaren konzept folgt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
ORP.3.A7	Schulung zur Vorgehensweise nach IT-Grundschutz			
	Umsetzungstatus: Teilweise	Umsetzung bis: 20.6.2024	Umsetzung durch:	
	Erläuterung:	Die Schulungen werden auf der Privatbasis durchgeführt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
ORP.3.A8	Messung und Auswertung des Lernerfolgs [Personalabteilung]			
	Umsetzungstatus: Nein	Umsetzung bis: 10.4.2024	Umsetzung durch:	
	Erläuterung:	Es gibt keine Messung und Auswertung des Lernerfolgs.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
CON.6	Löschen und Vernichten			R1
SWDS	Informationsverbund			
	Kompletter Standort der Werft			
CON.6.A2	Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen			
	Umsetzungstatus: Teilweise	Umsetzung bis: 2.8.2024	Umsetzung durch:	
	Erläuterung:	Die Daten werden durch löscherfahren vernichtet, aber papier etc nicht.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
CON.6.A4	Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern			
	Umsetzungstatus: Teilweise	Umsetzung bis: 3.7.2024	Umsetzung durch:	
	Erläuterung:	Es gibt keine geeignete Geräte und Werkzeuge für die Löscung alle eingesetzten Datenträgerarten.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:

CON.6	Löschen und Vernichten			R1
SWDS	Informationsverbund Kompletter Standort der Werft			
CON.6.A8	Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen [Mitarbeitende, IT-Betrieb, Datenschutzbeauftragte]			
	Umsetzungstatus: Nein	Umsetzung bis: 4.5.2024	Umsetzung durch:	
	Erläuterung:	Der System Administratot macht das mit Hilfe eines freeware tools.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
CON.6.A11	Löschen und Vernichtung von Datenträgern durch externe Dienstleistende			
	Umsetzungstatus: Nein	Umsetzung bis: 6.6.2024	Umsetzung durch:	
	Erläuterung:	Es gibt keinen Prozess zum Löschen und Vernichten durch externe Dienstleistende.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
CON.6.A12	Mindestanforderungen an Verfahren zur Löschen und Vernichtung			
	Umsetzungstatus: Nein	Umsetzung bis: 9.8.2024	Umsetzung durch:	
	Erläuterung:			
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
CON.9	Informationsaustausch			R3
SWDS	Informationsverbund Kompletter Standort der Werft			
CON.9.A1	Festlegung zulässiger Empfängender [Zentrale Verwaltung]			
	Umsetzungstatus: Nein	Umsetzung bis: 4.4.2024	Umsetzung durch:	
	Erläuterung:	Es gibt keine Sicherstellung, dass es durch die Weitergabe von Informationen nicht gegen rechtliche Rahmenbedingungen verstößen wird.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
CON.9.A2	Regelung des Informationsaustausches			
	Umsetzungstatus: Teilweise	Umsetzung bis: 5.5.2024	Umsetzung durch:	
	Erläuterung:	Der CEO hat dies entschieden, aber eher so in einer großen Gruppenleiterrunde. Allgemeiner Konsens ist, das keiner Informationen nach draußen geben darf, es sei denn der CEO erlaubt es.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:

CON.9	Informationsaustausch			R3
SWDS	Informationsverbund Kompletter Standort der Werft			
CON.9.A3	Unterweisung des Personals zum Informationsaustausch [Fachverantwortliche]			
Umsetzungstatus:	Nein	Umsetzung bis:	5.5.2024	Umsetzung durch:
Erläuterung:	Fachverantwortliche informieren die Mitarbeitenden über die Rahmenbedingungen jedes Informationsaustauschs nicht.			
Personalkosten	fix:	variabel:	pro:	
Sachkosten	fix:	variabel:	pro:	
CON.9.A4	Vereinbarungen zum Informationsaustausch mit Externen [Zentrale Verwaltung]			
Umsetzungstatus:	Nein	Umsetzung bis:	5.4.2024	Umsetzung durch:
Erläuterung:	Bei einem regelmäßigen Informationsaustausch mit anderen Institutionen vereinbart die Institution die Rahmenbedingungen für den Informationsaustausch formal nicht.			
Personalkosten	fix:	variabel:	pro:	
Sachkosten	fix:	variabel:	pro:	
CON.9.A5	Beseitigung von Restinformationen vor Weitergabe [Benutzende]			
Umsetzungstatus:	Teilweise	Umsetzung bis:	7.2.2023	Umsetzung durch:
Erläuterung:	Es wird teilweise über die Gefahren von Rest- und Zusatzinformationen in Dokumenten und Dateien vom Admin informiert.			
Personalkosten	fix:	variabel:	pro:	
Sachkosten	fix:	variabel:	pro:	
DER.4	Notfallmanagement			R3
SWDS	Informationsverbund Kompletter Standort der Werft			
DER.4.A2	Integration von Notfallmanagement und Informationssicherheitsmanagement [Informationssicherheitsbeauftragte (ISB)]			
Umsetzungstatus:	Nein	Umsetzung bis:	7.2.2023	Umsetzung durch:
Erläuterung:	Es besteht die Notwendigkeit, die Integration und Koordination dieser beiden Managementbereiche zu verbessern, um sicherzustellen, dass die Sicherheitsprozesse angemessen auf Sicherheitsvorfälle und Notfallsituationen reagieren können.			
Personalkosten	fix:	variabel:	pro:	
Sachkosten	fix:	variabel:	pro:	

Geschäftsprozesse

Anwendungen

APP.1.1	Office-Produkte	R2
A01	Excel Excel ermöglicht es den Mitarbeitern, umfangreiche Datenmengen aus Produktion und Vertrieb zu verarbeiten, zu analysieren und zu präsentieren. Excel wird für die Erstellung von Produktionsplänen, Verkaufsprognosen und Budgets genutzt.	Risikoanalyse erforderlich
APP.1.1.A3	Sicheres Öffnen von Dokumenten aus externen Quellen [Benutzende] Umsetzungstatus: Nein Umsetzung bis: NO DATE Umsetzung durch: Erläuterung: Die Dokumente aus externen Quellen werden nicht auf Schadsoftware überprüft. Personalkosten fix: variabel: pro: Sachkosten fix: variabel: pro:	
APP.1.1.A6	Testen neuer Versionen von Office-Produkten Umsetzungstatus: Nein Umsetzung bis: NO DATE Umsetzung durch: Erläuterung: Neue Versionen von Office-Produkten werden nicht vom Einsatz getestet. Personalkosten fix: variabel: pro: Sachkosten fix: variabel: pro:	
APP.1.1.A11	Geregelter Einsatz von Erweiterungen für Office-Produkte Umsetzungstatus: Nein Umsetzung bis: NO DATE Umsetzung durch: Erläuterung: Personalkosten fix: variabel: pro: Sachkosten fix: variabel: pro:	
APP.1.1.A14	Schutz gegen nachträgliche Veränderungen von Dokumenten [Benutzende] Umsetzungstatus: Teilweise Umsetzung bis: NO DATE Umsetzung durch: Erläuterung: Diese Information wird in der Schulung erwähnt aber nicht erprobt oder geprüft ob das durchgeführt wird. Personalkosten fix: variabel: pro: Sachkosten fix: variabel: pro:	
APP.1.1.A17	Sensibilisierung zu spezifischen Office-Eigenschaften Umsetzungstatus: Teilweise Umsetzung bis: NO DATE Umsetzung durch: Erläuterung: Wird im Rahmen der 30 Min. Schulung durchgeführt. Personalkosten fix: variabel: pro: Sachkosten fix: variabel: pro:	

OPS.1.2.5	Fernwartung	R3
A04	TeamViewer	Risikoanalyse erforderlich
Die Software ermöglicht es Benutzern, auf sichere Weise von verschiedenen Standorten aus auf Computer und andere Geräte zuzugreifen.		
OPS.1.2.5.A5	Einsatz von Online-Diensten	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	TeamViewer ist lokal installiert.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
OPS.1.2.5.A6	Erstellung einer Richtlinie für die Fernwartung	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Keine Richtlinie zur Fernwartung wurde erstellt.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
OPS.1.2.5.A7	Dokumentation bei der Fernwartung	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Die Dokumentation wird nur dann erstellt, wenn der server runtergefahren wird.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
OPS.1.2.5.A8	Sichere Protokolle bei der Fernwartung	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Die Teamviewer Protokolle sind im Einsatz.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
OPS.1.2.5.A9	Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Zur Beschaffung werden Fernwartungswerkzeuge eingesetzt, die auf dem Markt verfügbar sind.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:

OPS.1.2.5	Fernwartung	R3
A04	TeamViewer	Risikoanalyse erforderlich
Die Software ermöglicht es Benutzern, auf sichere Weise von verschiedenen Standorten aus auf Computer und andere Geräte zuzugreifen.		
OPS.1.2.5.A10	Umgang mit Fernwartungswerkzeugen	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Nur Admin darf mit den Fernwartungswerkzeugen arbeiten.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
OPS.1.2.5.A17	Authentisierungsmechanismen bei der Fernwartung	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt keine Mehr-Faktor-Verfahren zur Authentisierung.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
OPS.1.2.5.A19	Fernwartung durch Dritte	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt keine Maßnahmen für diesen Fall.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
OPS.1.2.5.A20	Betrieb der Fernwartung	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt keinen Meldeprozess für Support- und Fernwartungsanliegen, nur per Anruf.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
OPS.1.2.5.A21	Erstellung eines Notfallplans für den Ausfall der Fernwartung	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt keinen Notfallplan für den Ausfall der Fernwartung.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:

OPS.1.2.5	Fernwartung	R3
A04	TeamViewer	Risikoanalyse erforderlich
Die Software ermöglicht es Benutzern, auf sichere Weise von verschiedenen Standorten aus auf Computer und andere Geräte zuzugreifen.		
OPS.1.2.5.A24	Absicherung integrierter Fernwartungssysteme	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Es gibt keine Absicherung integrierter Fernwartungssysteme.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
OPS.1.2.5.A25	Entkopplung der Kommunikation bei der Fernwartung	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Kein Sprungserver wird dafür verwendet.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
APP.1.1	Office-Produkte	R2
A05	Word	Risikoanalyse erforderlich
Microsoft Word ist eine weit verbreitete Textverarbeitungssoftware, die von den Abteilungen Produktion und Vertrieb in unserem Unternehmen genutzt wird.		
APP.1.1.A3	Sicheres Öffnen von Dokumenten aus externen Quellen [Benutzende]	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Die Dokumente aus externen Quellen werden nicht auf Schadsoftware überprüft.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
APP.1.1.A6	Testen neuer Versionen von Office-Produkten	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Neue Versionen von Office-Produkten werden nicht vom Einsatz getestet.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
APP.1.1.A11	Geregelter Einsatz von Erweiterungen für Office-Produkte	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:

APP.1.1	Office-Produkte	R2
A05	Word	Risikoanalyse erforderlich
Microsoft Word ist eine weit verbreitete Textverarbeitungssoftware, die von den Abteilungen Produktion und Vertrieb in unserem Unternehmen genutzt wird.		
APP.1.1.A14	Schutz gegen nachträgliche Veränderungen von Dokumenten [Benutzende]	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Umsetzung durch:	
Erläuterung:	Diese Information wird in der schulung erwähnt aber nicht erprobt oder geprüft ob das durchgeführt wird.	
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
APP.1.1.A17	Sensibilisierung zu spezifischen Office-Eigenschaften	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Umsetzung durch:	
Erläuterung:	Wird im Rahmen der 30 Min. Schulung durchgeführt.	
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:

IT-Systeme

SYS.3.1	Laptops	R2
C1	Client Betrieb Laptop	Risikoanalyse erforderlich
SYS.3.1.A1 Regelungen zur mobilen Nutzung von Laptops		
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Umsetzung durch:	
Erläuterung:	Die Benutzenden werden auf die Regelungen zur mobilen Nutzung von Laptops innerhalb der 30 min Schulung hingewiesen.	
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
SYS.3.1.A3	Einsatz von Personal Firewalls	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Umsetzung durch:	
Erläuterung:	MacBooks haben keine firewall, die firewall kann durch Benutzer manipuliert werden.	
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
SYS.3.1.A7	Geregelte Übergabe und Rücknahme eines Laptops [Benutzende]	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
Erläuterung:	Diese Anforderung wurde nicht umgesetzt.	
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:

SYS.3.1	Laptops	R2
C1	Client Betrieb Laptop	Risikoanalyse erforderlich
SYS.3.1.A8	Sicherer Anschluss von Laptops an Datennetze [Benutzende]	
	Umsetzungstatus: Teilweise Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Dafür wird VPN Verbindung benutzt.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
SYS.3.1.A9	Sicherer Fernzugriff mit Laptops	
	Umsetzungstatus: Teilweise Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Es wird ein VPN verwendet, um ins Firmennetz zu kommen.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
SYS.3.1.A10	Abgleich der Datenbestände von Laptops [Benutzende]	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Die Laptops werden nie platt gemacht und es werden keine Daten gelöscht.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
SYS.3.1.A13	Verschlüsselung von Laptops	
	Umsetzungstatus: Teilweise Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: MacOS - ja, Windows - nicht.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
SYS.3.1.A14	Geeignete Aufbewahrung von Laptops [Benutzende]	
	Umsetzungstatus: Teilweise Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Die Benutzer werden dazu angehalten, ob sie dies tun. Es wird aber nicht überprüft, daher ist keine klare ja oder nein Aussage möglich.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
SYS.3.1.A15	Geeignete Auswahl von Laptops [Beschaffungsstelle]	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Nein, die Laptops werden einfach gekauft.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:

NET.3.1	Router und Switches			R2
HP1	Switch Betrieb			Risikoanalyse erforderlich
NET.3.1.A1	Sichere Grundkonfiguration eines Routers oder Switches			
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Es wird nur die Standardeinstellung verwendet. Diese ist bedingt sicher, nicht komplett schutzlos, sollte aber angepasst werden.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A4	Schutz der Administrationsschnittstellen			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Die Anforderung wurde nicht implementiert.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A5	Schutz vor Fragmentierungsangriffen			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Standardeinstellung bietet keinen richtigen Schutz.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A9	Betriebsdokumentationen			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Die Konfigurationsänderungen und sicherheitsrelevante Aufgaben werden nicht dokumentiert.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A10	Erstellung einer Sicherheitsrichtlinie			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A11	Beschaffung eines Routers oder Switches			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:

NET.3.1	Router und Switches			R2
HP1	Switch Betrieb			Risikoanalyse erforderlich
NET.3.1.A12	Erstellung einer Konfigurations-Checkliste für Router und Switches			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A13	Administration über ein gesondertes Managementnetz			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A14	Schutz vor Missbrauch von ICMP-Nachrichten			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A15	Bogon- und Spoofing-Filterung			
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Bogon- und Spoofing-Filterung wurde durch Standardeinstellung über Geräte-Konten implementiert.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A16	Schutz vor „IPv6 Routing Header Type-0“-Angriffen			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A17	Schutz vor DoS- und DDoS-Angriffen			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:

NET.3.1	Router und Switches	R2
HP1	Switch Betrieb	Risikoanalyse erforderlich
NET.3.1.A18	Einrichtung von Access Control Lists	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix:
	Sachkosten	fix:
NET.3.1.A19	Sicherung von Switch-Ports	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Für die Clients - nein, für Server - ja.
	Personalkosten	fix:
	Sachkosten	fix:
NET.3.1.A22	Notfallvorsorge bei Routern und Switches	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix:
	Sachkosten	fix:
NET.3.1.A23	Revision und Penetrationstests	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix:
	Sachkosten	fix:
HP2	Switch Produktion	Risikoanalyse erforderlich
NET.3.1.A1	Sichere Grundkonfiguration eines Routers oder Switches	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Es wird nur die Standardeinstellung verwendet. Diese ist bedingt sicher, nicht komplett schutzlos, sollte aber angepasst werden.
	Personalkosten	fix:
	Sachkosten	fix:

NET.3.1	Router und Switches			R2
HP2	Switch Produktion			Risikoanalyse erforderlich
NET.3.1.A4	Schutz der Administrationsschnittstellen			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Die Anforderung wurde nicht implementiert.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
NET.3.1.A5	Schutz vor Fragmentierungsangriffen			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Standardeinstellung bietet keinen richtigen Schutz.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
NET.3.1.A9	Betriebsdokumentationen			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Die Konfigurationsänderungen und sicherheitsrelevante Aufgaben werden nicht dokumentiert.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
NET.3.1.A10	Erstellung einer Sicherheitsrichtlinie			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Diese Anforderung wurde nicht umgesetzt.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
NET.3.1.A11	Beschaffung eines Routers oder Switches			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Diese Anforderung wurde nicht umgesetzt.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
NET.3.1.A12	Erstellung einer Konfigurations-Checkliste für Router und Switches			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Diese Anforderung wurde nicht umgesetzt.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:

NET.3.1	Router und Switches	R2
HP2	Switch Produktion	Risikoanalyse erforderlich
NET.3.1.A13	Administration über ein gesondertes Managementnetz	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Diese Anforderung wurde nicht umgesetzt.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
NET.3.1.A14	Schutz vor Missbrauch von ICMP-Nachrichten	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Diese Anforderung wurde nicht umgesetzt.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
NET.3.1.A15	Bogon- und Spoofing-Filterung	
	Umsetzungstatus: Teilweise Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Bogon- und Spoofing-Filterung wurde durch Standardeinstellung über Geräte-Konten implementiert.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
NET.3.1.A16	Schutz vor „IPv6 Routing Header Type-0“-Angriffen	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Diese Anforderung wurde nicht umgesetzt.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
NET.3.1.A17	Schutz vor DoS- und DDoS-Angriffen	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Diese Anforderung wurde nicht umgesetzt.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
NET.3.1.A18	Einrichtung von Access Control Lists	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Diese Anforderung wurde nicht umgesetzt.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:

NET.3.1	Router und Switches	R2
HP2	Switch Produktion	Risikoanalyse erforderlich
NET.3.1.A19	Sicherung von Switch-Ports	
Umsetzungstatus:	Teilweise	Umsetzung bis: NO DATE
Erläuterung:	Für die Clients - nein, für Server - ja.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
NET.3.1.A22	Notfallvorsorge bei Routern und Switches	
Umsetzungstatus:	Nein	Umsetzung bis: NO DATE
Erläuterung:	Diese Anforderung wurde nicht umgesetzt.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
NET.3.1.A23	Revision und Penetrationstests	
Umsetzungstatus:	Nein	Umsetzung bis: NO DATE
Erläuterung:	Diese Anforderung wurde nicht umgesetzt.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
R1	Router	Risikoanalyse erforderlich
NET.3.1.A1	Sichere Grundkonfiguration eines Routers oder Switches	
Umsetzungstatus:	Teilweise	Umsetzung bis: NO DATE
Erläuterung:	Es wird nur die Standardeinstellung verwendet. Diese ist bedingt sicher, nicht komplett schutzlos, sollte aber angepasst werden.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
NET.3.1.A4	Schutz der Administrationsschnittstellen	
Umsetzungstatus:	Nein	Umsetzung bis: NO DATE
Erläuterung:	Die Anforderung wurde nicht implementiert.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:

NET.3.1	Router und Switches			R2
R1	Router			Risikoanalyse erforderlich
NET.3.1.A5	Schutz vor Fragmentierungsangriffen			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Standardeinstellung bietet keinen richtigen Schutz.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A9	Betriebsdokumentationen			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Die Konfigurationsänderungen und sicherheitsrelevante Aufgaben werden nicht dokumentiert.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A10	Erstellung einer Sicherheitsrichtlinie			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A11	Beschaffung eines Routers oder Switches			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A12	Erstellung einer Konfigurations-Checkliste für Router und Switches			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:
NET.3.1.A13	Administration über ein gesondertes Managementnetz			
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.		
	Personalkosten	fix:	variabel:	pro:
	Sachkosten	fix:	variabel:	pro:

NET.3.1	Router und Switches	R2
R1	Router	Risikoanalyse erforderlich
NET.3.1.A14	Schutz vor Missbrauch von ICMP-Nachrichten	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:
NET.3.1.A15	Bogon- und Spoofing-Filterung	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Bogon- und Spoofing-Filterung wurde durch Standardeinstellung über Geräte-Konten implementiert.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:
NET.3.1.A16	Schutz vor „IPv6 Routing Header Type-0“-Angriffen	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:
NET.3.1.A17	Schutz vor DoS- und DDoS-Angriffen	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:
NET.3.1.A18	Einrichtung von Access Control Lists	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:
NET.3.1.A19	Sicherung von Switch-Ports	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Für die Clients - nein, für Server - ja.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:

NET.3.1	Router und Switches	R2
R1	Router	Risikoanalyse erforderlich
NET.3.1.A22	Notfallvorsorge bei Routern und Switches	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:
NET.3.1.A23	Revision und Penetrationstests	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:
SYS.1.1	Allgemeiner Server	R2
S1	Server Betrieb	Risikoanalyse erforderlich
SYS.1.1.A6	Deaktivierung nicht benötigter Dienste	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Der Server wird installiert und nur die benötigte software. Es werden also keine Änderungen an den Grundeinstellungen vorgenommen.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:
SYS.1.1.A9	Einsatz von Virenschutz-Programmen auf Servern	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Standard Viren Programm wurde dafür eingesetzt.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:
SYS.1.1.A11	Festlegung einer Sicherheitsrichtlinie für Server	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Die Anforderungen an Server werden in einer separaten Sicherheitsrichtlinie nicht konkretisiert.
	Personalkosten	fix: variabel:
	Sachkosten	fix: variabel:

SYS.1.1	Allgemeiner Server			R2
S1	Server Betrieb			Risikoanalyse erforderlich
SYS.1.1.A12	Planung des Server-Einsatzes			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Diese Anforderung wurde nicht umgesetzt.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
SYS.1.1.A13	Beschaffung von Servern			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Diese Anforderung wurde nicht umgesetzt.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
SYS.1.1.A16	Sichere Installation und Grundkonfiguration von Servern			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Diese Anforderung wurde nicht umgesetzt.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
SYS.1.1.A19	Einrichtung lokaler Paketfilter			
Umsetzungstatus:	Teilweise	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Einrichtung lokaler Paketfilter wurde teilweise umgesetzt.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
SYS.1.1.A21	Betriebsdokumentation für Server			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Es gibt keine Betriebsdokumentation.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:
SYS.1.1.A22	Einbindung in die Notfallplanung			
Umsetzungstatus:	Nein	Umsetzung bis:	NO DATE	Umsetzung durch:
Erläuterung:	Es gibt keinen Notfallplan.			
Personalkosten	fix:	variabel:		pro:
Sachkosten	fix:	variabel:		pro:

SYS.1.1	Allgemeiner Server	R2
S1	Server Betrieb	Risikoanalyse erforderlich
SYS.1.1.A23	Systemüberwachung und Monitoring von Servern	
Umsetzungstatus:	Nein	Umsetzung bis: NO DATE
Erläuterung:	Es gibt kein Konzept für Systemüberwachung und Monitoring von Servern.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
SYS.1.1.A24	Sicherheitsprüfungen für Server	
Umsetzungstatus:	Nein	Umsetzung bis: NO DATE
Erläuterung:	Server werden nicht gesondert geprüft.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
SYS.1.1.A25	Geregelte Außerbetriebnahme eines Servers	
Umsetzungstatus:	Nein	Umsetzung bis: NO DATE
Erläuterung:	Wenn nötig, aber es gibt keinen Wartungsplan.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
SYS.1.1.A35	Erstellung und Pflege eines Betriebshandbuchs	
Umsetzungstatus:	Nein	Umsetzung bis: NO DATE
Erläuterung:	Es gibt kein Betriebshandbuch.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
SYS.1.1.A37	Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten	
Umsetzungstatus:	Nein	Umsetzung bis: NO DATE
Erläuterung:	Es gibt keine Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:
SYS.1.1.A39	Zentrale Verwaltung der Sicherheitsrichtlinien von Servern	
Umsetzungstatus:	Nein	Umsetzung bis: NO DATE
Erläuterung:	Es gibt keine Zentrale Verwaltung der Sicherheitsrichtlinien von Servern.	Umsetzung durch:
Personalkosten	fix:	variabel:
Sachkosten	fix:	variabel:

SYS.1.1	Allgemeiner Server	R2
S2	Server Produktion	Risikoanalyse erforderlich
SYS.1.1.A6	Deaktivierung nicht benötigter Dienste	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Der Server wird installiert und nur die benötigte software. Es werden also keine Änderungen an den Grundeinstellungen vorgenommen.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A9	Einsatz von Virenschutz-Programmen auf Servern	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Standard Viren Programm wurde dafür eingesetzt.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A11	Festlegung einer Sicherheitsrichtlinie für Server	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Die Anforderungen an Server werden in einer separaten Sicherheitsrichtlinie nicht konkretisiert.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A12	Planung des Server-Einsatzes	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A13	Beschaffung von Servern	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A16	Sichere Installation und Grundkonfiguration von Servern	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Umsetzung durch:	
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:

SYS.1.1	Allgemeiner Server	R2
S2	Server Produktion	Risikoanalyse erforderlich
SYS.1.1.A19	Einrichtung lokaler Paketfilter	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
	Erläuterung:	Einrichtung lokaler Paketfilter wurde teilweise umgesetzt.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A21	Betriebsdokumentation für Server	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt keine Betriebsdokumentation.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A22	Einbindung in die Notfallplanung	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt keinen Notfallplan.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A23	Systemüberwachung und Monitoring von Servern	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt kein Konzept für Systemüberwachung und Monitoring von Servern.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A24	Sicherheitsprüfungen für Server	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Server werden nicht gesondert geprüft.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:
SYS.1.1.A25	Geregelte Außerbetriebnahme eines Servers	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Wenn nötig, aber es gibt keinen Wartungsplan.
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:

SYS.1.1	Allgemeiner Server	R2
S2	Server Produktion	Risikoanalyse erforderlich
SYS.1.1.A35	Erstellung und Pflege eines Betriebshandbuchs	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt kein Betriebshandbuch.
	Personalkosten	fix:
	Sachkosten	fix:
SYS.1.1.A37	Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt keine Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten.
	Personalkosten	fix:
	Sachkosten	fix:
SYS.1.1.A39	Zentrale Verwaltung der Sicherheitsrichtlinien von Servern	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Es gibt keine Zentrale Verwaltung der Sicherheitsrichtlinien von Servern.
	Personalkosten	fix:
	Sachkosten	fix:
SYS.1.2.3	Windows Server	R2
S1	Server Betrieb	Risikoanalyse erforderlich
SYS.1.2.3.A1	Planung von Windows Server	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Keine begründete und dokumentierte Entscheidung für eine geeignete Edition von Windows Server wird getroffen.
	Personalkosten	fix:
	Sachkosten	fix:
SYS.1.2.3.A2	Sichere Installation von Windows Server	
	Umsetzungstatus: Nein	Umsetzung bis: NO DATE
	Erläuterung:	Diese Anforderung wurde nicht umgesetzt, es gibt nur Standard Variante.
	Personalkosten	fix:
	Sachkosten	fix:

SYS.1.2.3	Windows Server	R2
S1	Server Betrieb	Risikoanalyse erforderlich
SYS.1.2.3.A3	Telemetrie- und Nutzungsdaten unter Windows Server	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Diese Anforderung wurde nicht umgesetzt.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
SYS.1.2.3.A5	Sichere Authentisierung und Autorisierung in Windows Server	
	Umsetzungstatus: Teilweise Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Nur Admin ist Motglied der Sicherheitsgruppe "Protected Users".	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
S2	Server Produktion	Risikoanalyse erforderlich
SYS.1.2.3.A1	Planung von Windows Server	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Keine begründete und dokumentierte Entscheidung für eine geeignete Edition von Windows Server wird getroffen.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
SYS.1.2.3.A2	Sichere Installation von Windows Server	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Diese Anforderung wurde nicht umgesetzt, es gibt nur Standard Variante.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:
SYS.1.2.3.A3	Telemetrie- und Nutzungsdaten unter Windows Server	
	Umsetzungstatus: Nein Umsetzung bis: NO DATE	Umsetzung durch:
	Erläuterung: Diese Anforderung wurde nicht umgesetzt.	
	Personalkosten fix:	variabel:
	Sachkosten fix:	variabel:

SYS.1.2.3	Windows Server	R2
S2	Server Produktion	Risikoanalyse erforderlich
SYS.1.2.3.A5	Sichere Authentisierung und Autorisierung in Windows Server	
	Umsetzungstatus: Teilweise	Umsetzung bis: NO DATE
		Umsetzung durch:
	Erläuterung:	Nur Admin ist Mitglied der Sicherheitsgruppe "Protected Users".
	Personalkosten	fix: variabel: pro:
	Sachkosten	fix: variabel: pro:

ICS-Systeme

Andere/IoT-Systeme

Kommunikationsverbindungen

Räume

Modernisierter BSI IT-Grundschutz: Auditbericht

Informationsverbund:	Informationsverbund
Abkürzung:	SWDS
Mitarbeiter:	35
Geltungsbereich:	Kompletter Standort der Werft
Datum:	23.01.2024, 22:18
Autor:	Gruppe 4
Version:	0.1
Freigabe:	Sebastian Breu
Vorgehensweise der Absicherung:	STANDARD

Informationsverbund

Baustein			
CON.6	Löschen und Vernichten	R1	2023-1
Beschreibung: -			
Umsetzung			
CON.6.A1	Regelung für die Löschung und Vernichtung von Informationen [Zentrale Verwaltung, Fachverantwortliche, Datenschutzbeauftragte, IT-Betrieb]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Könnten Sie bitte erläutern, wie die Regelung für die Löschung und Vernichtung von Informationen in der Werft aktuell umgesetzt wird und welche Rolle dabei die zentrale Verwaltung, die Fachverantwortlichen, der Datenschutzbeauftragte und der IT-Betrieb spielen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
CON.6.A11	Löschen und Vernichtung von Datenträgern durch externe Dienstleistende	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie erfolgt die Überprüfung externer Dienstleister hinsichtlich ihrer Verfahrensweisen zum sicheren Löschen und Vernichten?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.6.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
CON.6.A12	Mindestanforderungen an Verfahren zur Löschen und Vernichtung	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Maßnahmen ergreift die Institution, um sicherzustellen, dass Informationen sicher gelöscht oder vernichtet werden, bevor Fachverfahren, Geschäftsprozesse und IT-Systeme produktiv eingeführt werden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
CON.6.A13	Vernichtung defekter digitaler Datenträger	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie wird sichergestellt, dass Informationen auf digitalen wiederbeschreibbaren Datenträgern vollständig und sicher gelöscht werden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
CON.6.A2	Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie gewährleistet die Institution, dass Informationen auf Datenträgern sicher gelöscht oder vernichtet werden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 2.4.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
CON.6.A4	Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es klare Regelungen und Verfahrensweisen für die sichere Löschung und Vernichtung von Informationen in der Institution?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
CON.6.A8	Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen [Mitarbeitende, IT-Betrieb, Datenschutzbeauftragte]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es klare Regelungen und Verfahrensweisen für die sichere Löschung und Vernichtung von Informationen in der Institution?		Status: Korrekt Abweichung: Keine Behebungsfrist: 6.5.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Baustein			
CON.9	Informationsaustausch	R3	2023-1
Beschreibung: -			
Umsetzung			
CON.9.A1	Festlegung zulässiger Empfangender [Zentrale Verwaltung]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird es sichergestellt, dass durch die Weitergabe von Informationen nicht gegen rechtliche Rahmenbedingungen verstößen wird?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.4.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
CON.9.A2	Regelung des Informationsaustausches	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird es sichergestellt, dass wie die Informationen bei der Übertragung geschützt sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
CON.9.A3	Unterweisung des Personals zum Informationsaustausch [Fachverantwortliche]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Mitarbeitenden über die Rahmenbedingungen jedes Informationsaustauschs von Fachverantwortlichen informiert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.6.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
CON.9.A4	Vereinbarungen zum Informationsaustausch mit Externen [Zentrale Verwaltung]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden bei einem regelmäßigen Informationsaustausch mit anderen Institutionen die Institution die Rahmenbedingungen für den Informationsaustausch formal vereinbart?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 5.4.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
CON.9.A5	Beseitigung von Restinformationen vor Weitergabe [Benutzende]	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Informiert die Institution über die Gefahren von Rest- und Zusatzinformationen in Dokumenten und Dateien?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.6.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
CON.9.A6	Kompatibilitätsprüfung des Sende- und Empfangssystems	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird es überprüft, ob die eingesetzten IT-Systeme und Produkte kompatibel sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 5.4.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
CON.9.A7	Sicherungskopie der übermittelten Daten	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird eine Sicherungskopie der übermittelten Informationen erstellt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
CON.9.A8	Verschlüsselung und digitale Signatur	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird es überprüft, ob Informationen während des Austausches kryptografisch gesichert werden?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Baustein			
ORP.3	Sensibilisierung und Schulung zur Informationssicherheit	R1	2023-1
Beschreibung: -			
Umsetzung			
ORP.3.A1	Sensibilisierung der Institutionsleitung für Informationssicherheit [Vorgesetzte, Institutionsleitung]	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Schulungsmaßnahmen sind für alle Mitarbeiter verpflichtend, unabhängig von ihrem Sicherheitsbedarf?		Status: Korrekt Abweichung: Keine Behebungsfrist: 25.4.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
ORP.3.A3	Einweisung des Personals in den sicheren Umgang mit IT [Vorgesetzte, Personalabteilung, IT-Betrieb]	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie wird sichergestellt, dass alle Mitarbeiter grundlegende Kenntnisse über Informationssicherheit haben?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 18.4.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
ORP.3.A4	Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es gezielte Schulungen für bestimmte Abteilungen oder Teams, die spezifischen Sicherheitsanforderungen unterliegen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
ORP.3.A6	Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es regelmäßige Schulungen zu aktuellen Bedrohungen und Sicherheitspraktiken?			
Status: Korrekt			
Abweichung: Keine			
Behebungsfrist: 7.2.2023			
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
ORP.3.A7	Schulung zur Vorgehensweise nach IT-Grundschutz	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden IT-Grundschutz-Schulungen geplant?			
Status: Korrekt			
Abweichung: Keine			
Behebungsfrist: 7.2.2023			
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
ORP.3.A8	Messung und Auswertung des Lernerfolgs [Personalabteilung]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie werden die Schulungsprogrammen bei den Mitarbeiter ausgewertet?			
Status: Korrekt			
Abweichung: Keine			
Behebungsfrist: 21.3.2024			
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Geschäftsprozesse

Anwendungen

A01

Baustein			
APP.1.1	Office-Produkte	R2	2023-1
Beschreibung: -			
Umsetzung			
APP.1.1.A10	Regelung der Software-Entwicklung durch Endbenutzende	Umsetzungsstatus: Entbehrlich	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Maßnahmen sind geplant oder bereits implementiert, um die Software-Entwicklung durch Endbenutzer zu regulieren und sicherzustellen, dass sie den geltenden Richtlinien und Standards entspricht?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 15.10.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A11	Geregelter Einsatz von Erweiterungen für Office-Produkte	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Stellen Sie sicher, dass der geregelte Einsatz von Erweiterungen für Office-Produkte erfüllt wird?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 28.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
APP.1.1.A12	Verzicht auf Cloud-Speicherung [Benutzende]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Stellen Sie sicher, dass der Verzicht auf Cloud-Speicherung die Datenschutzziele, insbesondere Verfügbarkeit, Integrität, Verbindlichkeit, Wiederherstellbarkeit und Verschlüsselung, erfüllt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A13	Verwendung von Viewer-Funktionen [Benutzende]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird die Verwendung von Viewer-Funktionen beim Verwenden von Office-Produkten durch die Benutzer deaktiviert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A14	Schutz gegen nachträgliche Veränderungen von Dokumenten [Benutzende]	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Maßnahmen wurden ergriffen, um sicherzustellen, dass Dokumente vor nachträglichen Veränderungen geschützt sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 15.5.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
APP.1.1.A17	Sensibilisierung zu spezifischen Office-Eigenschaften	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Können Sie sicherstellen, dass alle Benutzer angemessen über die spezifischen Eigenschaften der Office-Anwendungen informiert und sensibilisiert werden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 21.6.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A2	Einschränken von Aktiven Inhalten	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie wird sichergestellt, dass die Ausführung von Aktiven Inhalten in den Office-Produkten eingeschränkt ist, und gibt es Mechanismen, um sicherzustellen, dass dies nur aus vertrauenswürdigen Quellen erfolgt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A3	Sicheres Öffnen von Dokumenten aus externen Quellen [Benutzende]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Können Sie uns die aktuellen Sicherheitsmaßnahmen und Richtlinien bezüglich des sicheren Öffnens von Dokumenten aus externen Quellen im Unternehmen erläutern?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 24.7.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
APP.1.1.A6	Testen neuer Versionen von Office-Produkten	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden neue Versionen von Office-Produkten vor dem produktiven Einsatz auf Kompatibilität mit etablierten Arbeitsmitteln wie Makros, Dokumentenvorlagen oder Formularen der Institution geprüft?		Status: Korrekt Abweichung: Keine Behebungsfrist: 20.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

A04

Baustein			
OPS.1.2.5	Fernwartung	R3	2023-1
Beschreibung: -			
Umsetzung			
OPS.1.2.5.A1	Planung des Einsatzes der Fernwartung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie wird die Fernwartung in unserer Institution geplant und durchgeführt?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
OPS.1.2.5.A10	Umgang mit Fernwartungswerkzeugen	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es Schulungsmaßnahmen und Musterabläufe für den Umgang mit Fernwartungswerkzeugen im Unternehmen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 13.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
OPS.1.2.5.A17	Authentisierungsmechanismen bei der Fernwartung	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie werden Authentisierungsmechanismen bei der Fernwartung umgesetzt, insbesondere im Hinblick auf Mehr-Faktor-Verfahren?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 18.7.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
OPS.1.2.5.A19	Fernwartung durch Dritte	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Maßnahmen werden ergriffen, wenn die Fernwartung von externen Dienstleistern durchgeführt wird?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 12.4.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
OPS.1.2.5.A2	Sicherer Verbindungsaufbau bei der Fernwartung von Clients [Benutzende]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Sicherheitsmechanismen sind implementiert, um den sicheren Verbindungsaufbau bei der Fernwartung von Clients zu gewährleisten?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
OPS.1.2.5.A20	Betrieb der Fernwartung	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 29.5.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Existiert ein Meldeprozess für Support- und Fernwartungsanliegen, und wie werden Angriffe erkannt und abgewehrt?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
OPS.1.2.5.A21	Erstellung eines Notfallplans für den Ausfall der Fernwartung	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es einen Notfallplan für den Ausfall der Fernwartung, und wie sind die Folgen eines solchen Ausfalls minimiert?		Status: Korrekt Abweichung: Keine Behebungsfrist: 23.5.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
OPS.1.2.5.A24	Absicherung integrierter Fernwartungssysteme	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie werden integrierte Fernwartungssysteme abgesichert und auf ihre Funktionen beschränkt?		Status: Korrekt Abweichung: Keine Behebungsfrist: 17.7.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
OPS.1.2.5.A25	Entkopplung der Kommunikation bei der Fernwartung	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind redundante Kommunikationsverbindungen für Fernwartungszugänge eingerichtet, insbesondere Out-Of-Band-Management?		Status: Korrekt Abweichung: Keine Behebungsfrist: 27.6.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
OPS.1.2.5.A3	Absicherung der Schnittstellen zur Fernwartung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie werden die Schnittstellen zur Fernwartung abgesichert und auf das notwendige Maß beschränkt?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
OPS.1.2.5.A5	Einsatz von Online-Diensten	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie werden Online-Dienste für die Fernwartung genutzt, und welche Sicherheitsvorkehrungen sind dabei implementiert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.10.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
OPS.1.2.5.A6	Erstellung einer Richtlinie für die Fernwartung	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Richtlinie zur Fernwartung, und sind alle Zuständigen darüber informiert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 26.7.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
OPS.1.2.5.A7	Dokumentation bei der Fernwartung	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie wird die Fernwartung in unserer Institution dokumentiert, und wo werden die relevanten Dokumente aufbewahrt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 16.5.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
OPS.1.2.5.A8	Sichere Protokolle bei der Fernwartung	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Protokolle werden bei der Fernwartung eingesetzt, und wie wird sichergestellt, dass sie sicher sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 17.4.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
OPS.1.2.5.A9	Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie erfolgt die Auswahl und Beschaffung von Fernwartungswerkzeugen, und welche Kriterien werden dabei berücksichtigt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 10.4.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

A05

Baustein			
APP.1.1	Office-Produkte	R2	2023-1
Beschreibung: -			

Umsetzung			
APP.1.1.A10	Regelung der Software-Entwicklung durch Endbenutzende	Umsetzungsstatus: Entbehrlich	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Maßnahmen sind geplant oder bereits implementiert, um die Software-Entwicklung durch Endbenutzer zu regulieren und sicherzustellen, dass sie den geltenden Richtlinien und Standards entspricht?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 15.10.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A11	Geregelter Einsatz von Erweiterungen für Office-Produkte	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Stellen Sie sicher, dass der geregelte Einsatz von Erweiterungen für Office-Produkte erfüllt wird?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 28.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A12	Verzicht auf Cloud-Speicherung [Benutzende]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Stellen Sie sicher, dass der Verzicht auf Cloud-Speicherung die Datenschutzziele, insbesondere Verfügbarkeit, Integrität, Verbindlichkeit, Wiederherstellbarkeit und Verschlüsselung, erfüllt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
APP.1.1.A13	Verwendung von Viewer-Funktionen [Benutzende]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird die Verwendung von Viewer-Funktionen beim Verwenden von Office-Produkten durch die Benutzer deaktiviert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A14	Schutz gegen nachträgliche Veränderungen von Dokumenten [Benutzende]	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Maßnahmen wurden ergriffen, um sicherzustellen, dass Dokumente vor nachträglichen Veränderungen geschützt sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 15.5.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A17	Sensibilisierung zu spezifischen Office-Eigenschaften	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Können Sie sicherstellen, dass alle Benutzer angemessen über die spezifischen Eigenschaften der Office-Anwendungen informiert und sensibilisiert werden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 21.6.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
APP.1.1.A2	Einschränken von Aktiven Inhalten	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie wird sichergestellt, dass die Ausführung von Aktiven Inhalten in den Office-Produkten eingeschränkt ist, und gibt es Mechanismen, um sicherzustellen, dass dies nur aus vertrauenswürdigen Quellen erfolgt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A3	Sicheres Öffnen von Dokumenten aus externen Quellen [Benutzende]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Können Sie uns die aktuellen Sicherheitsmaßnahmen und Richtlinien bezüglich des sicheren Öffnens von Dokumenten aus externen Quellen im Unternehmen erläutern?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 24.7.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
APP.1.1.A6	Testen neuer Versionen von Office-Produkten	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden neue Versionen von Office-Produkten vor dem produktiven Einsatz auf Kompatibilität mit etablierten Arbeitsmitteln wie Makros, Dokumentenvorlagen oder Formularen der Institution geprüft?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

IT-Systeme

C1 Client Betrieb Laptop

Baustein			
SYS.3.1	Laptops	R2	2023-1
Beschreibung: -			
Umsetzung			
SYS.3.1.A1	Regelungen zur mobilen Nutzung von Laptops	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es Regelungen für die mobile Nutzung von Laptops?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.3.1.A10	Abgleich der Datenbestände von Laptops [Benutzende]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist der Prozess für die Übernahme von Daten von Laptops in den Informationsverbund der Institution geregelt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.3.1.A11	Sicherstellung der Energieversorgung von Laptops [Benutzende]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es Ersatzakkus?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.3.1.A12	Verlustmeldung für Laptops [Benutzende]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Welche Meldewege sind in der Institution etabliert, um den Verlust oder Diebstahl eines Laptops umgehend zu melden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.3.1.A13	Verschlüsselung von Laptops	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind die in Laptops verbaute Datenträger wie Festplatten oder SSDs verschlüsselt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.3.1.A14	Geeignete Aufbewahrung von Laptops [Benutzende]	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind Laptops außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.3.1.A15	Geeignete Auswahl von Laptops [Beschaffungsstelle]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Bevor Laptops beschafft werden, eine Anforderungsanalyse durchgeführt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.3.1.A3	Einsatz von Personal Firewalls	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist auf allen Laptops eine Personal Firewall aktiv, wenn sie außerhalb des Unternehmensnetzwerks genutzt werden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.3.1.A6	Sicherheitsrichtlinien für Laptops	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Sicherheitsrichtlinie für die Nutzung von Laptops im Unternehmen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.3.1.A7	Geregelte Übergabe und Rücknahme eines Laptops [Benutzende]	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist die sichere Übergabe und Rücknahme von Laptops geregelt, wenn diese von verschiedenen Personen genutzt werden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.3.1.A8	Sicherer Anschluss von Laptops an Datennetze [Benutzende]	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist der sichere Anschluss von Laptops an eigene oder fremde Datennetze und das Internet geregelt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.3.1.A9	Sicherer Fernzugriff mit Laptops	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wie wird sichergestellt, dass Benutzer nur über sichere Kommunikationskanäle auf das interne Netz der Institution zugreifen, wenn sie öffentliche Netze verwenden?		Status: Korrekt Abweichung: Keine Behebungsfrist: 20.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

HP1 Switch Betrieb			
Baustein			
NET.3.1	Router und Switches	R2	2023-1
Beschreibung: -			
Umsetzung			
NET.3.1.A1	Sichere Grundkonfiguration eines Routers oder Switches	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Sind die Konfigurationsänderungen nachvollziehbar dokumentiert und gesichert? 2.Laufen nur erforderliche Dienste? 3.Sind NICHT erforderliche Dienste deaktiviert/deinstalliert? 4.Gibt es unbenutzte Netz Ports? 5.Gibt es funktionale Erweiterungen? 6.Sind unnötige Auskunftsdiene		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A10	Erstellung einer Sicherheitsrichtlinie	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Sicherheitsrichtlinie für den Betrieb von Router und Switchen? Werden Veränderungen der Sicherheitsrichtlinie dokumentiert? Wird die Sicherheitsrichtlinie regelmäßig auf Korrektheit überprüft? Werden die Ergebnisse der Überprüfung der Sicherheitsrichtlinie dokumentiert?			Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A11	Beschaffung eines Routers oder Switches	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Anforderungsliste basierend auf der Sicherheitsrichtlinie?			Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A12	Erstellung einer Konfigurations-Checkliste für Router und Switches	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Konfigurations-Checkliste für die Einstellung von Routern und Switches?			Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A13	Administration über ein gesondertes Managementnetz	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden Router und Switche über ein separates Managementnetz administriert? Sind alle In-Band Administrationsschnittstellen deaktiviert? Sind die Managementprotokolle zur Authentisierung, Integritäts sicherung und Verschlüsselung aktiviert? Sind alle unsicheren Managementprotokolle deaktiviert?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A14	Schutz vor Missbrauch von ICMP-Nachrichten	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Protokolle ICMP und ICMPv6 restriktiv gefiltert?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A15	Bogon- und Spoofing-Filterung	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1. Werden gefälschter, reservierter oder noch nicht zugewiesener IP-Adressen welche in die Router und Switches eindringen können gefiltert?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A16	Schutz vor „IPv6 Routing Header Type-0“-Angriffen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es Maßnahmen gegen „IPv6 Routing Header Type-0“-Angriffen?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A17	Schutz vor DoS- und DDoS-Angriffen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es Maßnahmen gegen hochvolumige Angriffe sowie TCP-State-Exhaustion Angriffe?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A18	Einrichtung von Access Control Lists	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist der Zugriff auf Routern und Switches mithilfe von einer Access Control List definiert? a.Falls nicht: Wird der restriktivere Whitelist-Ansatz verwendet?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A19	Sicherung von Switch-Ports	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Ports eines Switches vor unberechtigten Zugriffen geschützt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A20	Sicherheitsaspekte von Routing-Protokollen	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Authentisieren sich Router, wenn sie Routing-Informationen austauschen oder Updates für Routing-Tabellen verschieben? Werden Dynamische Routing-Protokolle SOLLTEN ausschließlich in sicheren Netzen verwendet? Falls demilitarisierte Zone: Werden ausschließlich statische Routen eingetragen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A21	Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind alle Router und Switches an ein zentrales Identitäts- und Berechtigungsmanagement angebunden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A22	Notfallvorsorge bei Routern und Switches	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es einen Plan für die Fehlerdiagnose von Routern und Switches? Gibt es ein Plan um solche Fehler zu beheben? Gibt es Handlungsanweisungen für typische Ausfallszenarien? Orientiert sich die Notfallplanung am Notfallvorsorgekonzept? Ist das Notfallvorsorgekonzept in Papierform vorhanden? Wird das Konzept regelmäßig geprobt?	Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024		
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A23	Revision und Penetrationstests	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden Router und Switches SOLLTEN regelmäßig auf bekannte Sicherheitsprobleme überprüft? Werden regelmäßig Revisionen durchgeführt? Werden die Ergebnisse nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen? Werden Abweichungen nachgegangen?	Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024		
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A4	Schutz der Administrationsschnittstellen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Sind die Administrationszugänge auf einzelne IP-Agrarbereiche eingeschränkt? 2.Werden für Administrierung und Überwachung verschlüsselte Protokolle verwendet? 3.Gibt es unverschlüsselte Protokolle? a.Wird dafür ein eigenes Administrationsnetz verwendet? 4.Werden Managementschnittstellen und Administrationsverbindungen durch eine separate Firewall geschützt? 5.Gibt es Zeitbeschränkungen für z.B.: Timeouts? 6.Sind alle Dienste welche nicht für das Management-Interface benötigt werden deaktiviert? 7.Gibt es eine Hardwareschnittstelle welche nicht vor unberechtigten Zugriff geschützt ist?		Status: Korrekt	Abweichung: Keine
Nachbesserung erfolgt: Nein	Nachbesserung: -	Behebungsfrist: 3.3.2024	
Umsetzung			
NET.3.1.A5	Schutz vor Fragmentierungsangriffen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind an Router und Layer-3-Switch Schutzmechanismen aktiviert, um IPv4- sowie IPv6 Fragmentierungsangriffe abzuwehren?		Status: Korrekt	Abweichung: Keine
Nachbesserung erfolgt: Nein	Nachbesserung: -	Behebungsfrist: 3.3.2024	

Umsetzung			
NET.3.1.A6	Notfallzugriff auf Router und Switches	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Ist es dem Administrator möglich direkt auf Router/ Switches zuzugreifen?		Status: Korrekt	
			Abweichung: Keine
			Behebungsfrist: 3.3.2024
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A7	Protokollierung bei Routern und Switches	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Protokollieren Router/Switch z.B.: Reboots, Systemfehler, Konfig. Änderungen etc.?		Status: Korrekt	
			Abweichung: Keine
			Behebungsfrist: 3.3.2024
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A8	Regelmäßige Datensicherung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Wird eine regelmäßige Sicherung der Konfigurationsdatei durchgeführt? 2.Ist die Konfigurationsdatei im Notfall zugänglich?		Status: Korrekt	
			Abweichung: Keine
			Behebungsfrist: 3.3.2024
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A9	Betriebsdokumentationen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Werden die wichtigsten betrieblichen Aufgaben eines Routers oder Switches dokumentiert? 2.Wird die Dokumentation vor unbefugten Zugriffen geschützt?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

HP2			
Switch Produktion			
Baustein			
NET.3.1	Router und Switches	R2	2023-1
Beschreibung: -			
Umsetzung			
NET.3.1.A1	Sichere Grundkonfiguration eines Routers oder Switches	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Sind die Konfigurationsänderungen nachvollziehbar dokumentiert und gesichert? 2.Laufen nur erforderliche Dienste? 3.Sind NICHT erforderliche Dienste deaktiviert/deinstalliert? 4.Gibt es unbenutzte Netz Ports? 5.Gibt es funktionale Erweiterungen? 6.Sind unnötige Auskunftsdiene		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A10	Erstellung einer Sicherheitsrichtlinie	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Sicherheitsrichtlinie für den Betrieb von Router und Switchen? Werden Veränderungen der Sicherheitsrichtlinie dokumentiert? Wird die Sicherheitsrichtlinie regelmäßig auf Korrektheit überprüft? Werden die Ergebnisse der Überprüfung der Sicherheitsrichtlinie dokumentiert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A11	Beschaffung eines Routers oder Switches	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Anforderungsliste basierend auf der Sicherheitsrichtlinie?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A12	Erstellung einer Konfigurations-Checkliste für Router und Switches	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Konfigurations-Checkliste für die Einstellung von Routern und Switches?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A13	Administration über ein gesondertes Managementnetz	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden Router und Switche über ein separates Managementnetz administriert? Sind alle In-Band Administrationsschnittstellen deaktiviert? Sind die Managementprotokolle zur Authentisierung, Integritäts sicherung und Verschlüsselung aktiviert? Sind alle unsicheren Managementprotokolle deaktiviert?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A14	Schutz vor Missbrauch von ICMP-Nachrichten	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Protokolle ICMP und ICMPv6 restriktiv gefiltert?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A15	Bogon- und Spoofing-Filterung	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1. Werden gefälschter, reservierter oder noch nicht zugewiesener IP-Adressen welche in die Router und Switches eindringen können gefiltert?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A16	Schutz vor „IPv6 Routing Header Type-0“-Angriffen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es Maßnahmen gegen „IPv6 Routing Header Type-0“-Angriffen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A17	Schutz vor DoS- und DDoS-Angriffen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es Maßnahmen gegen hochvolumige Angriffe sowie TCP-State-Exhaustion Angriffe?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A18	Einrichtung von Access Control Lists	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist der Zugriff auf Routern und Switches mithilfe von einer Access Control List definiert? a.Falls nicht: Wird der restriktivere Whitelist-Ansatz verwendet?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A19	Sicherung von Switch-Ports	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Ports eines Switches vor unberechtigten Zugriffen geschützt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A20	Sicherheitsaspekte von Routing-Protokollen	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Authentisieren sich Router, wenn sie Routing-Informationen austauschen oder Updates für Routing-Tabellen verschießen? Werden Dynamische Routing-Protokolle SOLLTEN ausschließlich in sicheren Netzen verwendet? Falls demilitarisierte Zone: Werden ausschließlich statische Routen eingetragen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A21	Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind alle Router und Switches an ein zentrales Identitäts- und Berechtigungsmanagement angebunden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A22	Notfallvorsorge bei Routern und Switches	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es einen Plan für die Fehlerdiagnose von Routern und Switches? Gibt es ein Plan um solche Fehler zu beheben? Gibt es Handlungsanweisungen für typische Ausfallszenarien? Orientiert sich die Notfallplanung am Notfallvorsorgekonzept? Ist das Notfallvorsorgekonzept in Papierform vorhanden? Wird das Konzept regelmäßig geprobt?	Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024		
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A23	Revision und Penetrationstests	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden Router und Switches SOLLTEN regelmäßig auf bekannte Sicherheitsprobleme überprüft? Werden regelmäßig Revisionen durchgeführt? Werden die Ergebnisse nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen? Werden Abweichungen nachgegangen?	Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024		
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A4	Schutz der Administrationsschnittstellen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Sind die Administrationszugänge auf einzelne IP-Agrarbereiche eingeschränkt? 2.Werden für Administrierung und Überwachung verschlüsselte Protokolle verwendet? 3.Gibt es unverschlüsselte Protokolle? a.Wird dafür ein eigenes Administrationsnetz verwendet? 4.Werden Managementschnittstellen und Administrationsverbindungen durch eine separate Firewall geschützt? 5.Gibt es Zeitbeschränkungen für z.B.: Timeouts? 6.Sind alle Dienste welche nicht für das Management-Interface benötigt werden deaktiviert? 7.Gibt es eine Hardwareschnittstelle welche nicht vor unberechtigten Zugriff geschützt ist?		Status: Korrekt	Abweichung: Keine
Nachbesserung erfolgt: Nein		Nachbesserung: -	
Umsetzung			
NET.3.1.A5	Schutz vor Fragmentierungsangriffen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind an Router und Layer-3-Switch Schutzmechanismen aktiviert, um IPv4- sowie IPv6 Fragmentierungsangriffe abzuwehren?		Status: Korrekt	Abweichung: Keine
Nachbesserung erfolgt: Nein		Nachbesserung: -	

Umsetzung			
NET.3.1.A6	Notfallzugriff auf Router und Switches	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Ist es dem Administrator möglich direkt auf Router/ Switches zuzugreifen?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A7	Protokollierung bei Routern und Switches	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Protokollieren Router/Switch z.B.: Reboots, Systemfehler, Konfig. Änderungen etc.?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A8	Regelmäßige Datensicherung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Wird eine regelmäßige Sicherung der Konfigurationsdatei durchgeführt? 2.Ist die Konfigurationsdatei im Notfall zugänglich?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A9	Betriebsdokumentationen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Werden die wichtigsten betrieblichen Aufgaben eines Routers oder Switches dokumentiert? 2.Wird die Dokumentation vor unbefugten Zugriffen geschützt?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

R1 Router			
Baustein			
NET.3.1	Router und Switches	R2	2023-1
Beschreibung: -			
Umsetzung			
NET.3.1.A1	Sichere Grundkonfiguration eines Routers oder Switches	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Sind die Konfigurationsänderungen nachvollziehbar dokumentiert und gesichert? 2.Laufen nur erforderliche Dienste? 3.Sind NICHT erforderliche Dienste deaktiviert/deinstalliert? 4.Gibt es unbenutzte Netz Ports? 5.Gibt es funktionale Erweiterungen? 6.Sind unnötige Auskunftsdiene		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A10	Erstellung einer Sicherheitsrichtlinie	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Sicherheitsrichtlinie für den Betrieb von Router und Switchen? Werden Veränderungen der Sicherheitsrichtlinie dokumentiert? Wird die Sicherheitsrichtlinie regelmäßig auf Korrektheit überprüft? Werden die Ergebnisse der Überprüfung der Sicherheitsrichtlinie dokumentiert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A11	Beschaffung eines Routers oder Switches	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Anforderungsliste basierend auf der Sicherheitsrichtlinie?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A12	Erstellung einer Konfigurations-Checkliste für Router und Switches	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es eine Konfigurations-Checkliste für die Einstellung von Routern und Switches?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A13	Administration über ein gesondertes Managementnetz	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden Router und Switche über ein separates Managementnetz administriert? Sind alle In-Band Administrationsschnittstellen deaktiviert? Sind die Managementprotokolle zur Authentisierung, Integritäts sicherung und Verschlüsselung aktiviert? Sind alle unsicheren Managementprotokolle deaktiviert?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A14	Schutz vor Missbrauch von ICMP-Nachrichten	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Protokolle ICMP und ICMPv6 restriktiv gefiltert?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A15	Bogon- und Spoofing-Filterung	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1. Werden gefälschter, reservierter oder noch nicht zugewiesener IP-Adressen welche in die Router und Switches eindringen können gefiltert?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A16	Schutz vor „IPv6 Routing Header Type-0“-Angriffen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es Maßnahmen gegen „IPv6 Routing Header Type-0“-Angriffen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A17	Schutz vor DoS- und DDoS-Angriffen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es Maßnahmen gegen hochvolumige Angriffe sowie TCP-State-Exhaustion Angriffe?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A18	Einrichtung von Access Control Lists	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist der Zugriff auf Routern und Switches mithilfe von einer Access Control List definiert? a.Falls nicht: Wird der restriktivere Whitelist-Ansatz verwendet?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A19	Sicherung von Switch-Ports	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Ports eines Switches vor unberechtigten Zugriffen geschützt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A20	Sicherheitsaspekte von Routing-Protokollen	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Authentisieren sich Router, wenn sie Routing-Informationen austauschen oder Updates für Routing-Tabellen verschieben? Werden Dynamische Routing-Protokolle SOLLTEN ausschließlich in sicheren Netzen verwendet? Falls demilitarisierte Zone: Werden ausschließlich statische Routen eingetragen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A21	Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind alle Router und Switches an ein zentrales Identitäts- und Berechtigungsmanagement angebunden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A22	Notfallvorsorge bei Routern und Switches	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es einen Plan für die Fehlerdiagnose von Routern und Switches? Gibt es ein Plan um solche Fehler zu beheben? Gibt es Handlungsanweisungen für typische Ausfallszenarien? Orientiert sich die Notfallplanung am Notfallvorsorgekonzept? Ist das Notfallvorsorgekonzept in Papierform vorhanden? Wird das Konzept regelmäßig geprobt?	Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024		
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A23	Revision und Penetrationstests	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden Router und Switches SOLLTEN regelmäßig auf bekannte Sicherheitsprobleme überprüft? Werden regelmäßig Revisionen durchgeführt? Werden die Ergebnisse nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen? Werden Abweichungen nachgegangen?	Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024		
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A4	Schutz der Administrationsschnittstellen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Sind die Administrationszugänge auf einzelne IP-Agrarbereiche eingeschränkt? 2.Werden für Administrierung und Überwachung verschlüsselte Protokolle verwendet? 3.Gibt es unverschlüsselte Protokolle? a.Wird dafür ein eigenes Administrationsnetz verwendet? 4.Werden Managementschnittstellen und Administrationsverbindungen durch eine separate Firewall geschützt? 5.Gibt es Zeitbeschränkungen für z.B.: Timeouts? 6.Sind alle Dienste welche nicht für das Management-Interface benötigt werden deaktiviert? 7.Gibt es eine Hardwareschnittstelle welche nicht vor unberechtigten Zugriff geschützt ist?		Status: Korrekt	Abweichung: Keine
Nachbesserung erfolgt: Nein	Nachbesserung: -	Behebungsfrist: 3.3.2024	
Umsetzung			
NET.3.1.A5	Schutz vor Fragmentierungsangriffen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind an Router und Layer-3-Switch Schutzmechanismen aktiviert, um IPv4- sowie IPv6 Fragmentierungsangriffe abzuwehren?		Status: Korrekt	Abweichung: Keine
Nachbesserung erfolgt: Nein	Nachbesserung: -	Behebungsfrist: 3.3.2024	

Umsetzung			
NET.3.1.A6	Notfallzugriff auf Router und Switches	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Ist es dem Administrator möglich direkt auf Router/ Switches zuzugreifen?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A7	Protokollierung bei Routern und Switches	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Protokollieren Router/Switch z.B.: Reboots, Systemfehler, Konfig. Änderungen etc.?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
NET.3.1.A8	Regelmäßige Datensicherung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Wird eine regelmäßige Sicherung der Konfigurationsdatei durchgeführt? 2.Ist die Konfigurationsdatei im Notfall zugänglich?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
NET.3.1.A9	Betriebsdokumentationen	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: 1.Werden die wichtigsten betrieblichen Aufgaben eines Routers oder Switches dokumentiert? 2.Wird die Dokumentation vor unbefugten Zugriffen geschützt?		Status: Korrekt Abweichung: Keine Behebungsfrist: 3.3.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

S1 Server Betrieb			
Baustein			
SYS.1.1	Allgemeiner Server	R2	2023-1
Beschreibung: -			
Umsetzung			
SYS.1.1.A1	Zugriffsschutz und Nutzung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind physische Server an Orten betrieben, zu denen nur berechtigte Personen Zutritt haben?		Status: Korrekt Abweichung: Keine Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A10	Protokollierung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle sicherheitsrelevanten Systemereignisse protokolliert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A11	Festlegung einer Sicherheitsrichtlinie für Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind gemäß der allgemeinen Sicherheitsrichtlinie der Institution die Anforderungen an Server in einer separaten Sicherheitsrichtlinie konkretisiert, wird diese regelmäßig geprüft und die Ergebnisse der Prüfung dokumentiert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A12	Planung des Server-Einsatzes	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wurden mindestens folgende Punkte im Plan für die Server-Systeme berücksichtigt: Auswahl der Plattform (Hardware oder virtualisierte Ressourcen), des Betriebssystems und der Anwendungssoftware, Dimensionierung der Hardware (Leistung, Speicher, Bandbreite etc.), Art und Anzahl der Kommunikationsschnittstellen, Leistungsaufnahme, Wärmelast, Platzbedarf und Bauform, administrative Zugänge (siehe SYS.1.1.A5 Schutz von Schnittstellen), Zugriffe von Benutzenden, Protokollierung (siehe SYS.1.1.A10 Protokollierung), Aktualisierung von Betriebssystem und Anwendungen sowie Einbindung ins System- und Netzmanagement, in die Datensicherung und die Schutzsysteme (Virenschutz, IDS, etc.) ?		Status: Korrekt	Abweichung: Keine
Nachbesserung erfolgt: Nein	Nachbesserung: -	Behebungsfrist: 4.2.2024	
Umsetzung			
SYS.1.1.A13	Beschaffung von Servern	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wurde vor der Anschaffung der Server eine Anforderungsliste erstellt, anhand derer die am Markt erhältlichen Produkte bewertet wurden?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A15	Unterbrechungsfreie und stabile Stromversorgung [Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind alle Server an eine unterbrechungsfreie Stromversorgung angeschlossen?		Status: Korrekt Abweichung: Keine Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A16	Sichere Installation und Grundkonfiguration von Servern	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind vollständige Installations- und Konfigurationsvorgänge soweit wie möglich innerhalb einer gesonderten und von Produktivsystemen abgetrennten Installationsumgebung vorzunehmen?		Status: Korrekt Abweichung: Keine Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A19	Einrichtung lokaler Paketfilter	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist das vorhandene lokale Paketfilter über ein Regelwerk so ausgestaltet, dass die eingehende und ausgehende Kommunikation auf die erforderlichen Kommunikationspartner, Kommunikationsprotokolle sowie Ports und Schnittstellen beschränkt wird?		Status: Korrekt Abweichung: Keine Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A2	Authentisierung an Servern	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird der Zugriff auf Ressourcen und Konfigurationen von virtualisierten Servern auf berechtigte Personen begrenzt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A21	Betriebsdokumentation für Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird alles, was automatisiert dokumentiert werden kann, auch automatisiert dokumentiert und wenn ja, werden diese Dokumentationen vor unbefugtem Zugriff sowie Verlust geschützt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A22	Einbindung in die Notfallplanung	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Server im Notfallmanagementprozess berücksichtigt ?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A23	Systemüberwachung und Monitoring von Servern	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist das Server-System in einen geeigneten Systemüberwachungs- oder Monitoringkonzept eingebunden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A24	Sicherheitsprüfungen für Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Server regelmäßig Sicherheitstests unterzogen und werden diese nach Möglichkeit automatisiert, mittels geeigneter Skripte, durchgeführt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A25	Geregelte Außerbetriebnahme eines Servers	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist sichergestellt, dass bei einer Außerbetriebnahme eines Servers keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen oder schutzbedürftige Daten zurückbleiben?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A35	Erstellung und Pflege eines Betriebshandbuchs	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es ein Betriebshandbuch in dem alle erforderlichen Regelungen, Anforderungen und Einstellungen dokumentiert werden, die erforderlich sind, um Server zu betreiben und wird dieses regelmäßig aktualisiert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A37	Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind Anwendungen (insbesondere sicherheitskritische) und Betriebssystemkomponenten gemäß ihrem Schutzbedarf entsprechend besonders gekapselt oder gegenüber anderen Anwendungen und Betriebssystemkomponenten isoliert, um sowohl den unberechtigten Zugriff auf das Betriebssystem oder andere Anwendungen bei Angriffen als auch den Zugriff vom Betriebssystem auf besonders schützenswerte Dateien zu verhindern?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A39	Zentrale Verwaltung der Sicherheitsrichtlinien von Servern	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Einstellungen der Server durch Nutzung eines zentralen Managementsystems verwaltet und entsprechend dem ermittelten Schutzbedarf sowie auf den internen Richtlinien basierend konfiguriert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A5	Schutz von Schnittstellen	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind alle nicht verwendeten Schnittstellen für Wechselspeicher deaktiviert und ist es gewährleistet, dass nur vorgesehene Wechselspeicher/sonstige Geräte an die Server angeschlossen werden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A6	Deaktivierung nicht benötigter Dienste	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind alle nicht benötigten Serverrollen, Features und Funktionen, Firmware Funktionen, sonstige Software und Dienste deaktiviert oder deinstalliert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A9	Einsatz von Virenschutz-Programmen auf Servern	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden Virus-Schutzprogramme genutzt und wurde im Vorfeld geprüft, ob diese eingesetzt werden sollen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Baustein			
SYS.1.2.3	Windows Server	R2	2023-1
Beschreibung: -			
Umsetzung			
SYS.1.2.3.A1	Planung von Windows Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird es eine begründete und dokumentierte Entscheidung für eine geeignete Edition von Windows Server getroffen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.2.3.A2	Sichere Installation von Windows Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wurde die Server-Core-Variante installiert und wenn nein, wurde dies begründet?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.2.3.A3	Telemetrie- und Nutzungsdaten unter Windows Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wurde die Server-Core-Variante installiert und wenn nein, wurde dies begründet?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.2.3.A4	Schutz vor Ausnutzung von Schwachstellen in Anwendungen	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind Maßnahmen zum Schutz vor Exploits für alle Programme und Dienste aktiviert, die den Exploitsschutz von Windows unterstützen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.2.3.A5	Sichere Authentisierung und Autorisierung in Windows Server	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind in Windows Server alle Konten von Benutzenden Mitglied der Sicherheitsgruppe „Protected Users“?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.2.3.A6	Sicherheit beim Fernzugriff über RDP	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist die Gruppe der Berechtigten und IT-Systeme für den Remote-Desktopzugriff (RDP) durch die Zuweisung entsprechender Berechtigungen festgelegt?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

S2 Server Produktion			
Baustein			
SYS.1.1	Allgemeiner Server	R2	2023-1
Beschreibung: -			
Umsetzung			
SYS.1.1.A1	Zugriffsschutz und Nutzung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind physische Server an Orten betrieben, zu denen nur berechtigte Personen Zutritt haben?		Status: Korrekt Abweichung: Keine Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A10	Protokollierung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle sicherheitsrelevanten Systemereignisse protokolliert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A11	Festlegung einer Sicherheitsrichtlinie für Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind gemäß der allgemeinen Sicherheitsrichtlinie der Institution die Anforderungen an Server in einer separaten Sicherheitsrichtlinie konkretisiert, wird diese regelmäßig geprüft und die Ergebnisse der Prüfung dokumentiert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A12	Planung des Server-Einsatzes	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wurden mindestens folgende Punkte im Plan für die Server-Systeme berücksichtigt: Auswahl der Plattform (Hardware oder virtualisierte Ressourcen), des Betriebssystems und der Anwendungssoftware, Dimensionierung der Hardware (Leistung, Speicher, Bandbreite etc.), Art und Anzahl der Kommunikationsschnittstellen, Leistungsaufnahme, Wärmelast, Platzbedarf und Bauform, administrative Zugänge (siehe SYS.1.1.A5 Schutz von Schnittstellen), Zugriffe von Benutzenden, Protokollierung (siehe SYS.1.1.A10 Protokollierung), Aktualisierung von Betriebssystem und Anwendungen sowie Einbindung ins System- und Netzmanagement, in die Datensicherung und die Schutzsysteme (Virenschutz, IDS, etc.) ?		Status: Korrekt	Abweichung: Keine
Nachbesserung erfolgt: Nein	Nachbesserung: -	Behebungsfrist: 4.2.2024	
Umsetzung			
SYS.1.1.A13	Beschaffung von Servern	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wurde vor der Anschaffung der Server eine Anforderungsliste erstellt, anhand derer die am Markt erhältlichen Produkte bewertet wurden?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A15	Unterbrechungsfreie und stabile Stromversorgung [Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind alle Server an eine unterbrechungsfreie Stromversorgung angeschlossen?		Status: Korrekt Abweichung: Keine Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A16	Sichere Installation und Grundkonfiguration von Servern	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind vollständige Installations- und Konfigurationsvorgänge soweit wie möglich innerhalb einer gesonderten und von Produktivsystemen abgetrennten Installationsumgebung vorzunehmen?		Status: Korrekt Abweichung: Keine Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A19	Einrichtung lokaler Paketfilter	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist das vorhandene lokale Paketfilter über ein Regelwerk so ausgestaltet, dass die eingehende und ausgehende Kommunikation auf die erforderlichen Kommunikationspartner, Kommunikationsprotokolle sowie Ports und Schnittstellen beschränkt wird?		Status: Korrekt Abweichung: Keine Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A2	Authentisierung an Servern	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird der Zugriff auf Ressourcen und Konfigurationen von virtualisierten Servern auf berechtigte Personen begrenzt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A21	Betriebsdokumentation für Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird alles, was automatisiert dokumentiert werden kann, auch automatisiert dokumentiert und wenn ja, werden diese Dokumentationen vor unbefugtem Zugriff sowie Verlust geschützt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A22	Einbindung in die Notfallplanung	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Server im Notfallmanagementprozess berücksichtigt ?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A23	Systemüberwachung und Monitoring von Servern	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist das Server-System in einen geeigneten Systemüberwachungs- oder Monitoringkonzept eingebunden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A24	Sicherheitsprüfungen für Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden die Server regelmäßig Sicherheitstests unterzogen und werden diese nach Möglichkeit automatisiert, mittels geeigneter Skripte, durchgeführt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A25	Geregelte Außerbetriebnahme eines Servers	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist sichergestellt, dass bei einer Außerbetriebnahme eines Servers keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen oder schutzbedürftige Daten zurückbleiben?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A35	Erstellung und Pflege eines Betriebshandbuchs	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Gibt es ein Betriebshandbuch in dem alle erforderlichen Regelungen, Anforderungen und Einstellungen dokumentiert werden, die erforderlich sind, um Server zu betreiben und wird dieses regelmäßig aktualisiert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A37	Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind Anwendungen (insbesondere sicherheitskritische) und Betriebssystemkomponenten gemäß ihrem Schutzbedarf entsprechend besonders gekapselt oder gegenüber anderen Anwendungen und Betriebssystemkomponenten isoliert, um sowohl den unberechtigten Zugriff auf das Betriebssystem oder andere Anwendungen bei Angriffen als auch den Zugriff vom Betriebssystem auf besonders schützenswerte Dateien zu verhindern?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A39	Zentrale Verwaltung der Sicherheitsrichtlinien von Servern	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Einstellungen der Server durch Nutzung eines zentralen Managementsystems verwaltet und entsprechend dem ermittelten Schutzbedarf sowie auf den internen Richtlinien basierend konfiguriert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.1.A5	Schutz von Schnittstellen	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind alle nicht verwendeten Schnittstellen für Wechselspeicher deaktiviert und ist es gewährleistet, dass nur vorgesehene Wechselspeicher/sonstige Geräte an die Server angeschlossen werden?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A6	Deaktivierung nicht benötigter Dienste	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind alle nicht benötigten Serverrollen, Features und Funktionen, Firmware Funktionen, sonstige Software und Dienste deaktiviert oder deinstalliert?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.1.A9	Einsatz von Virenschutz-Programmen auf Servern	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden Virus-Schutzprogramme genutzt und wurde im Vorfeld geprüft, ob diese eingesetzt werden sollen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 4.2.2024	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Baustein			
SYS.1.2.3	Windows Server	R2	2023-1
Beschreibung: -			
Umsetzung			
SYS.1.2.3.A1	Planung von Windows Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wird es eine begründete und dokumentierte Entscheidung für eine geeignete Edition von Windows Server getroffen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.2.3.A2	Sichere Installation von Windows Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wurde die Server-Core-Variante installiert und wenn nein, wurde dies begründet?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.2.3.A3	Telemetrie- und Nutzungsdaten unter Windows Server	Umsetzungsstatus: Nein	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Wurde die Server-Core-Variante installiert und wenn nein, wurde dies begründet?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.2.3.A4	Schutz vor Ausnutzung von Schwachstellen in Anwendungen	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind Maßnahmen zum Schutz vor Exploits für alle Programme und Dienste aktiviert, die den Exploitsschutz von Windows unterstützen?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
SYS.1.2.3.A5	Sichere Authentisierung und Autorisierung in Windows Server	Umsetzungsstatus: Teilweise	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind in Windows Server alle Konten von Benutzenden Mitglied der Sicherheitsgruppe „Protected Users“?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
SYS.1.2.3.A6	Sicherheit beim Fernzugriff über RDP	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Ist die Gruppe der Berechtigten und IT-Systeme für den Remote-Desktopzugriff (RDP) durch die Zuweisung entsprechender Berechtigungen festgelegt?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

ICS-Systeme

Andere/IoT-Systeme

Netzwerke

Räume

EG-1	Büroraum Geschäftsleiter		
Baustein			
INF.7	Büroarbeitsplatz	R2	2023-1
Beschreibung: -			

Umsetzung			
INF.7.A1	Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden nur geeignete Räume als Büroräume genutzt, die dem Schutzbedarf der verarbeiteten Informationen angemessen sind? Ist die Arbeitsstättenverordnung bei der Auswahl und Einrichtung der Büroräume umgesetzt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Fenster geschlossen, wenn Mitarbeitende ihre Büroräume verlassen, insbesondere wenn sich vertrauliche Informationen im Raum befinden? Werden Türen abgeschlossen, wenn der Büroräum verlassen wird, besonders in Bereichen mit Publikumsverkehr?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A3	Fliegende Verkabelung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Befinden sich Stromanschlüsse und Zugänge zum Datennetz im Büroräum dort, wo IT-Geräte aufgestellt sind? Sind Verkabelungen, die über den Boden verlaufen, geeignet abgedeckt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind die Arbeitsplätze ergonomisch eingerichtet, insbesondere die Bildschirme? Wird darauf geachtet, dass Bildschirme so aufgestellt sind, dass ein ergonomisches und ungestörtes Arbeiten möglich ist?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Mitarbeitenden dazu angehalten, ihren Arbeitsplatz aufgeräumt zu hinterlassen? Werden Arbeitsplätze sorgfältig überprüft, um sicherzustellen, dass keine vertraulichen Informationen frei zugänglich sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden vertrauliche Dokumente und Datenträger verschlossen aufbewahrt, wenn sie nicht verwendet werden? Gibt es geeignete Behältnisse in den Büroräumen oder in deren Umfeld für die Aufbewahrung?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

EG-2

Büroraum Personal**Baustein**

INF.7

Büroarbeitsplatz

R2

2023-1

Beschreibung: -

Umsetzung

INF.7.A1

Geeignete Auswahl und Nutzung eines
Büroraumes [Vorgesetzte]

Umsetzungsstatus: Ja

Umsetzungsstatus aus Maßnahme ableiten:
Nein

Beschreibung: -

Audit am: 10.1.2024

Auditor: -

Befragte(r): -

Prüfmethoden: Interviews

Prüffragen: Werden nur geeignete Räume als Büroräume genutzt, die dem Schutzbedarf der verarbeiteten Informationen angemessen sind? Ist die Arbeitsstättenverordnung bei der Auswahl und Einrichtung der Büroräume umgesetzt?

Status: Korrekt

Abweichung: Keine

Behebungsfrist: 7.2.2023

Nachbesserung erfolgt: Nein

Nachbesserung: -

Umsetzung

INF.7.A2

Geschlossene Fenster und abgeschlossene
Türen [Mitarbeitende, Haustechnik]

Umsetzungsstatus: Ja

Umsetzungsstatus aus Maßnahme ableiten:
Nein

Beschreibung: -

Audit am: 7.2.2023

Auditor: -

Befragte(r): -

Prüfmethoden: Interviews

Prüffragen: Werden alle Fenster geschlossen, wenn Mitarbeitende ihre Büroräume verlassen, insbesondere wenn sich vertrauliche Informationen im Raum befinden? Werden Türen abgeschlossen, wenn der Büraum verlassen wird, besonders in Bereichen mit Publikumsverkehr?

Status: Korrekt

Abweichung: Keine

Behebungsfrist: 7.2.2023

Nachbesserung erfolgt: Nein

Nachbesserung: -

Umsetzung			
INF.7.A3	Fliegende Verkabelung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Befinden sich Stromanschlüsse und Zugänge zum Datennetz im Bürraum dort, wo IT-Geräte aufgestellt sind? Sind Verkabelungen, die über den Boden verlaufen, geeignet abgedeckt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind die Arbeitsplätze ergonomisch eingerichtet, insbesondere die Bildschirme? Wird darauf geachtet, dass Bildschirme so aufgestellt sind, dass ein ergonomisches und ungestörtes Arbeiten möglich ist?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Mitarbeitenden dazu angehalten, ihren Arbeitsplatz aufgeräumt zu hinterlassen? Werden Arbeitsplätze sorgfältig überprüft, um sicherzustellen, dass keine vertraulichen Informationen frei zugänglich sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden vertrauliche Dokumente und Datenträger verschlossen aufbewahrt, wenn sie nicht verwendet werden? Gibt es geeignete Behältnisse in den Büroräumen oder in deren Umfeld für die Aufbewahrung?			
Status: Korrekt			
Abweichung: Keine			
Behebungsfrist: 7.2.2023			
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Büroraum Entwicklung			
Baustein			
INF.7	Büroarbeitsplatz	R2	2023-1
Beschreibung: -			
Umsetzung			
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Fenster geschlossen, wenn Mitarbeitende ihre Büroräume verlassen, insbesondere wenn sich vertrauliche Informationen im Raum befinden? Werden Türen abgeschlossen, wenn der Büraum verlassen wird, besonders in Bereichen mit Publikumsverkehr?			
Status: Korrekt			
Abweichung: Keine			
Behebungsfrist: 7.2.2023			
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A3	Fliegende Verkabelung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Befinden sich Stromanschlüsse und Zugänge zum Datennetz im Bürraum dort, wo IT-Geräte aufgestellt sind? Sind Verkabelungen, die über den Boden verlaufen, geeignet abgedeckt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind die Arbeitsplätze ergonomisch eingerichtet, insbesondere die Bildschirme? Wird darauf geachtet, dass Bildschirme so aufgestellt sind, dass ein ergonomisches und ungestörtes Arbeiten möglich ist?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Mitarbeitenden dazu angehalten, ihren Arbeitsplatz aufgeräumt zu hinterlassen? Werden Arbeitsplätze sorgfältig überprüft, um sicherzustellen, dass keine vertraulichen Informationen frei zugänglich sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden vertrauliche Dokumente und Datenträger verschlossen aufbewahrt, wenn sie nicht verwendet werden? Gibt es geeignete Behältnisse in den Büroräumen oder in deren Umfeld für die Aufbewahrung?			
Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023			
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Büroraum Einkauf			
Baustein			
INF.7	Büroarbeitsplatz	R2	2023-1
Beschreibung: -			
Umsetzung			
INF.7.A1	Geeignete Auswahl und Nutzung eines Büorraumes [Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden nur geeignete Räume als Büoräume genutzt, die dem Schutzbedarf der verarbeiteten Informationen angemessen sind? Ist die Arbeitsstättenverordnung bei der Auswahl und Einrichtung der Büoräume umgesetzt?			
Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023			
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Fenster geschlossen, wenn Mitarbeitende ihre Büroräume verlassen, insbesondere wenn sich vertrauliche Informationen im Raum befinden? Werden Türen abgeschlossen, wenn der Büraum verlassen wird, besonders in Bereichen mit Publikumsverkehr?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A3	Fliegende Verkabelung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Befinden sich Stromanschlüsse und Zugänge zum Datennetz im Büraum dort, wo IT-Geräte aufgestellt sind? Sind Verkabelungen, die über den Boden verlaufen, geeignet abgedeckt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind die Arbeitsplätze ergonomisch eingerichtet, insbesondere die Bildschirme? Wird darauf geachtet, dass Bildschirme so aufgestellt sind, dass ein ergonomisches und ungestörtes Arbeiten möglich ist?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Mitarbeitenden dazu angehalten, ihren Arbeitsplatz aufgeräumt zu hinterlassen? Werden Arbeitsplätze sorgfältig überprüft, um sicherzustellen, dass keine vertraulichen Informationen frei zugänglich sind?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden vertrauliche Dokumente und Datenträger verschlossen aufbewahrt, wenn sie nicht verwendet werden? Gibt es geeignete Behältnisse in den Büroräumen oder in deren Umfeld für die Aufbewahrung?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

LG-1 Büroraum Produktion			
Baustein			
INF.7	Büroarbeitsplatz	R2	2023-1
Beschreibung: -			

Umsetzung			
INF.7.A1	Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden nur geeignete Räume als Büroräume genutzt, die dem Schutzbedarf der verarbeiteten Informationen angemessen sind? Ist die Arbeitsstättenverordnung bei der Auswahl und Einrichtung der Büroräume umgesetzt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Fenster geschlossen, wenn Mitarbeitende ihre Büroräume verlassen, insbesondere wenn sich vertrauliche Informationen im Raum befinden? Werden Türen abgeschlossen, wenn der Büroräum verlassen wird, besonders in Bereichen mit Publikumsverkehr?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A3	Fliegende Verkabelung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Befinden sich Stromanschlüsse und Zugänge zum Datennetz im Büroräum dort, wo IT-Geräte aufgestellt sind? Sind Verkabelungen, die über den Boden verlaufen, geeignet abgedeckt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind die Arbeitsplätze ergonomisch eingerichtet, insbesondere die Bildschirme? Wird darauf geachtet, dass Bildschirme so aufgestellt sind, dass ein ergonomisches und ungestörtes Arbeiten möglich ist?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Mitarbeitenden dazu angehalten, ihren Arbeitsplatz aufgeräumt zu hinterlassen? Werden Arbeitsplätze sorgfältig überprüft, um sicherzustellen, dass keine vertraulichen Informationen frei zugänglich sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden vertrauliche Dokumente und Datenträger verschlossen aufbewahrt, wenn sie nicht verwendet werden? Gibt es geeignete Behältnisse in den Büroräumen oder in deren Umfeld für die Aufbewahrung?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

OG-1

Büroraum Vertrieb

Baustein

INF.7

Büroarbeitsplatz

R2

2023-1

Beschreibung: -

Umsetzung

INF.7.A1

Geeignete Auswahl und Nutzung eines
Büroraumes [Vorgesetzte]

Umsetzungsstatus: Ja

Umsetzungsstatus aus Maßnahme ableiten:
Nein

Beschreibung: -

Audit am: 10.1.2024

Auditor: -

Befragte(r): -

Prüfmethoden: Interviews

Prüffragen: Werden nur geeignete Räume als Büroräume genutzt, die dem Schutzbedarf der verarbeiteten Informationen angemessen sind? Ist die Arbeitsstättenverordnung bei der Auswahl und Einrichtung der Büroräume umgesetzt?

Status: Korrekt

Abweichung: Keine

Behebungsfrist: 7.2.2023

Nachbesserung erfolgt: Nein

Nachbesserung: -

Umsetzung

INF.7.A2

Geschlossene Fenster und abgeschlossene
Türen [Mitarbeitende, Haustechnik]

Umsetzungsstatus: Ja

Umsetzungsstatus aus Maßnahme ableiten:
Nein

Beschreibung: -

Audit am: 7.2.2023

Auditor: -

Befragte(r): -

Prüfmethoden: Interviews

Prüffragen: Werden alle Fenster geschlossen, wenn Mitarbeitende ihre Büroräume verlassen, insbesondere wenn sich vertrauliche Informationen im Raum befinden? Werden Türen abgeschlossen, wenn der Büraum verlassen wird, besonders in Bereichen mit Publikumsverkehr?

Status: Korrekt

Abweichung: Keine

Behebungsfrist: 7.2.2023

Nachbesserung erfolgt: Nein

Nachbesserung: -

Umsetzung			
INF.7.A3	Fliegende Verkabelung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Befinden sich Stromanschlüsse und Zugänge zum Datennetz im Bürraum dort, wo IT-Geräte aufgestellt sind? Sind Verkabelungen, die über den Boden verlaufen, geeignet abgedeckt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind die Arbeitsplätze ergonomisch eingerichtet, insbesondere die Bildschirme? Wird darauf geachtet, dass Bildschirme so aufgestellt sind, dass ein ergonomisches und ungestörtes Arbeiten möglich ist?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Mitarbeitenden dazu angehalten, ihren Arbeitsplatz aufgeräumt zu hinterlassen? Werden Arbeitsplätze sorgfältig überprüft, um sicherzustellen, dass keine vertraulichen Informationen frei zugänglich sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden vertrauliche Dokumente und Datenträger verschlossen aufbewahrt, wenn sie nicht verwendet werden? Gibt es geeignete Behältnisse in den Büroräumen oder in deren Umfeld für die Aufbewahrung?			
Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023			
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Büroraum IT Admin			
Baustein			
INF.7	Büroarbeitsplatz	R2	2023-1
Beschreibung: -			
Umsetzung			
INF.7.A1	Geeignete Auswahl und Nutzung eines Büorraumes [Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden nur geeignete Räume als Büoräume genutzt, die dem Schutzbedarf der verarbeiteten Informationen angemessen sind? Ist die Arbeitsstättenverordnung bei der Auswahl und Einrichtung der Büoräume umgesetzt?			
Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023			
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Fenster geschlossen, wenn Mitarbeitende ihre Büroräume verlassen, insbesondere wenn sich vertrauliche Informationen im Raum befinden? Werden Türen abgeschlossen, wenn der Büraum verlassen wird, besonders in Bereichen mit Publikumsverkehr?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A3	Fliegende Verkabelung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Befinden sich Stromanschlüsse und Zugänge zum Datennetz im Büraum dort, wo IT-Geräte aufgestellt sind? Sind Verkabelungen, die über den Boden verlaufen, geeignet abgedeckt?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind die Arbeitsplätze ergonomisch eingerichtet, insbesondere die Bildschirme? Wird darauf geachtet, dass Bildschirme so aufgestellt sind, dass ein ergonomisches und ungestörtes Arbeiten möglich ist?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Mitarbeitenden dazu angehalten, ihren Arbeitsplatz aufgeräumt zu hinterlassen? Werden Arbeitsplätze sorgfältig überprüft, um sicherzustellen, dass keine vertraulichen Informationen frei zugänglich sind?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden vertrauliche Dokumente und Datenträger verschlossen aufbewahrt, wenn sie nicht verwendet werden? Gibt es geeignete Behältnisse in den Büroräumen oder in deren Umfeld für die Aufbewahrung?		Status: Korrekt Abweichung: Keine Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

OG-3 Büroraum CISO			
Baustein			
INF.7	Büroarbeitsplatz	R2	2023-1
Beschreibung: -			

Umsetzung			
INF.7.A1	Geeignete Auswahl und Nutzung eines Büroraumes [Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 10.1.2024	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden nur geeignete Räume als Büroräume genutzt, die dem Schutzbedarf der verarbeiteten Informationen angemessen sind? Ist die Arbeitsstättenverordnung bei der Auswahl und Einrichtung der Büroräume umgesetzt?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A2	Geschlossene Fenster und abgeschlossene Türen [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Fenster geschlossen, wenn Mitarbeitende ihre Büroräume verlassen, insbesondere wenn sich vertrauliche Informationen im Raum befinden? Werden Türen abgeschlossen, wenn der Büroräum verlassen wird, besonders in Bereichen mit Publikumsverkehr?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A3	Fliegende Verkabelung	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Befinden sich Stromanschlüsse und Zugänge zum Datennetz im Büroräum dort, wo IT-Geräte aufgestellt sind? Sind Verkabelungen, die über den Boden verlaufen, geeignet abgedeckt?		Status: Korrekt	Abweichung: Keine
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

Umsetzung			
INF.7.A5	Ergonomischer Arbeitsplatz [Zentrale Verwaltung, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Sind die Arbeitsplätze ergonomisch eingerichtet, insbesondere die Bildschirme? Wird darauf geachtet, dass Bildschirme so aufgestellt sind, dass ein ergonomisches und ungestörtes Arbeiten möglich ist?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A6	Aufgeräumter Arbeitsplatz [Mitarbeitende, Vorgesetzte]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden alle Mitarbeitenden dazu angehalten, ihren Arbeitsplatz aufgeräumt zu hinterlassen? Werden Arbeitsplätze sorgfältig überprüft, um sicherzustellen, dass keine vertraulichen Informationen frei zugänglich sind?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		
Umsetzung			
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger [Mitarbeitende, Haustechnik]	Umsetzungsstatus: Ja	Umsetzungsstatus aus Maßnahme ableiten: Nein
Beschreibung: -			
Audit am: 7.2.2023	Auditor: -	Befragte(r): -	Prüfmethoden: Interviews
Prüffragen: Werden vertrauliche Dokumente und Datenträger verschlossen aufbewahrt, wenn sie nicht verwendet werden? Gibt es geeignete Behältnisse in den Büroräumen oder in deren Umfeld für die Aufbewahrung?		Status: Korrekt	
		Abweichung: Keine	
		Behebungsfrist: 7.2.2023	
Nachbesserung erfolgt: Nein	Nachbesserung: -		

IT-Sicherheitskonzept

IT-Sicherheitskonzept zum 23.01.2024

Verantwortlich erstellt von

Alona Vasylchenko
Jewgeni Sikorski
Tobia Wübben

mit

Sebastian Breu

23.01.2024

HTW - Projekt im Rahmen des Moduls:
Informationssicherheit
Dozent: Sebastian Breu

Inhaltsverzeichnis

1	Einleitung	2
1.1	Einführung	2
1.2	Revisionsnachweis	4
1.3	Ansprechpartner	4
1.4	Begrifflichkeiten	5
1.5	Weiterführende bzw. ergänzende Dokumente	5
2	Allgemeines	6
2.1	Methodik	6
2.2	Geltungsbereich und Verantwortlichkeiten	7
2.3	Gesetzliche Vorgaben dieses Verfahrens (Compliance)	9
2.4	Personenbezogene Daten	10
3	Strukturanalyse (Ist-Aufnahme)	11
3.1	Gruppierung	11
3.2	Relevante Geschäftsprozesse und dazugehörige Informationen	16
3.3	Relevante Anwendungen und dazugehörige Informationen	16
3.3.1	Zuordnung Geschäftsprozesse zu Anwendungen	17
3.3.2	Technologieübersicht der einzelnen Anwendungen	17
3.4	Netzplan	18
3.1	IT-Systeme, ICS-Systeme, IoT-Geräte	19
3.2	Kommunikationspfade	20
3.3	Betrachtung der Räume	21
4	Schutzbedarfsfeststellung	25
4.1	Definition der Schutzbedarfskategorien	25
4.1.1	Schutzziele	25
4.1.2	Schadenskategorien	25
4.1.3	Individualisierte Schutzbedarfskategorien	26
4.2	Schutzbedarfsfeststellung Geschäftsprozesse	30
4.3	Schutzbedarfsfeststellung Anwendungen	32
4.4	Schutzbedarfsfeststellung IT-Systeme	34
4.5	Schutzbedarfsfeststellung Kommunikationsverbindungen	39
5	Modellierung des Informationsverbunds	44
5.1	Modellierung der IT-Systeme (Bausteine „alter“ Grundschutz)	44
6	IT-Grundschutz-Check	46
7	Risikoanalyse	46

Abbildungsverzeichnis

Abbildung 1: Netzplan 18

Tabellenverzeichnis

Tabelle 1: Revisionsnachweis	4
Tabelle 2: Weiterführende Dokumente.....	5
Tabelle 4: Anwendungen	17
Tabelle 10: Räume	24
Tabelle 11: Individuelle Schutzbedarfskategorien.....	29
Tabelle 12: Schutzbedarfsfeststellung Geschäftsprozesse	31
Tabelle 13: Schutzbedarfsfeststellung Anwendungen	33
Tabelle 14: Schutzbedarfsfeststellung IT-Systeme	37

1 Einleitung

Die Motivation für die Erstellung dieses Konzepts liegt in der Notwendigkeit, eine sichere und resiliente IT-Infrastruktur zu gewährleisten, die den laufenden Betrieb unterstützt und gleichzeitig Compliance-Anforderungen erfüllt. Es zielt darauf ab, potenzielle Sicherheitslücken zu identifizieren, präventive Maßnahmen zur Risikominderung zu empfehlen und einen strategischen Plan für den Umgang mit Sicherheitsvorfällen zu entwickeln.

In den folgenden Abschnitten wird eine detaillierte Analyse von **Ships-Without-Diesel-Solution** vorgestellt, um die spezifischen Sicherheitsanforderungen zu verstehen. Dies umfasst eine Untersuchung der aktuellen IT-Landschaft, der vorhandenen Sicherheitsmaßnahmen und der potenziellen Bedrohungsszenarien. Durch dieses Verständnis wird es möglich sein, maßgeschneiderte Sicherheitsstrategien und -richtlinien zu entwickeln, die nicht nur den aktuellen, sondern auch zukünftigen Sicherheitsanforderungen gerecht werden.

Die Erstellung dieses Konzepts ist ein entscheidender Schritt zur Gewährleistung der Integrität, Verfügbarkeit und Vertraulichkeit der IT-Systeme von **Ships-Without-Diesel-Solution**. Es spiegelt unser Engagement für Sicherheit und Datenschutz wider und dient als Leitfaden für kontinuierliche Verbesserungen in einem sich ständig verändernden Sicherheitsumfeld.

1.1 Einführung

Unser Unternehmen, **Ships-Without-Diesel-Solution**, ist ein führender Akteur in der Branche Schiffsbau bekannt für unsere Expertise in der Entwicklung von Schiffen welche auf Diesel verzichten. Seit unserer Gründung im Jahr 2000 haben wir uns stetig weiterentwickelt und sind stolz darauf, eine Schlüsselrolle in dem Schiffsbau zu spielen, indem wir innovative Lösungen und Dienstleistungen anbieten, die auf die Bedürfnisse unserer Kunden zugeschnitten sind.

Mit Sitz in Berlin bedienen wir sowohl lokale als auch internationale Kunden, wobei wir besonderen Wert auf Qualität, Kundenservice, Innovation legen. Unser Portfolio umfasst eine breite Palette von Schiffsbaulösungen, die darauf abzielen, spezifische Probleme oder Bedürfnisse der Branche zu lösen.

Die Unternehmenskultur von **Ships-Without-Diesel-Solution** ist geprägt von Innovation, Nachhaltigkeit, Kundenorientierung. Diese Werte spiegeln sich in jedem Aspekt unserer Arbeit wider und sind die Grundlage für unseren anhaltenden Erfolg und unser Engagement für Exzellenz. Unser Team besteht aus hochqualifizierten Fachleuten, die sich der Bereitstellung außergewöhnlicher Ergebnisse und der Förderung kontinuierlicher Verbesserungen verpflichtet fühlen.

Die Sicherheit unserer Informationssysteme und die Gewährleistung des Datenschutzes sind von entscheidender Bedeutung für unseren Betrieb und unsere Reputation. Daher ist dieses

Einleitung

IT-Sicherheitskonzept ein wesentlicher Bestandteil unserer Strategie, um sicherzustellen, dass wir die besten Praktiken in der IT-Sicherheit befolgen und unsere Kunden, Mitarbeiter und Geschäftspartner effektiv schützen.

In den folgenden Abschnitten dieses Konzepts werden wir detaillierter auf die spezifischen Herausforderungen und Anforderungen in Bezug auf die IT-Sicherheit eingehen, die für unser Unternehmen relevant sind. Durch dieses Verständnis können Außenstehende besser nachvollziehen, warum und wie wir bestimmte Sicherheitsmaßnahmen implementieren, um die Integrität und Vertraulichkeit unserer Daten und Systeme zu gewährleisten.

1.2 Revisionsnachweis

VERSION	ÄNDERUNG BZW. REVISION	BEARBEITER	DATUM
0.1	Initialerstellung	Auditoren	23.01.2024
1.0			

Tabelle 1: Revisionsnachweis

1.3 Ansprechpartner

Ansprechpartner für Fragen oder Bemerkungen bzgl. dieses IT-Sicherheitskonzept sind:

CISO
Ciso@swds.de
1234/5678

und

Sebastian Breu
Breu@swds.de
1234/5678 -1

1.4 Begrifflichkeiten

Sollten einige Spezifische Begriffe in Ihrem Verbund vorkommen sollten Sie dem Außenstehenden Leser hier eine Übersicht und Erklärung zu diesen Begriffen liefern. Hierzu bietet sich der Verweis auf ein zusätzliches Dokument, welches als Anlage geschaffen wird, hin.

Eine Übersicht der verwendeten Begriffe und deren Erklärungen befinden sich in der Anlage Begriffserklärung falls vorhanden.

1.5 Weiterführende bzw. ergänzende Dokumente

Führen Sie hier alle Dokumente auf die im Kontext zum IT-Sicherheitskonzept gelten

Begriffserklärungen	Enthält eine Übersicht über alle Begrifflichkeiten, Kontext des IT-Sicherheitskonzepts verwendet werden.
Datenschutzkonzept*	Das Datenschutzkonzept des Unternehmens
Risikoanalyse	Analyse der Risiken nach BSI Standard 200-3
Netzwerkplan	Übersicht über die Netzwerkarchitektur des Unternehmens
Organigramm	Eine Übersicht der Belegschaft
Sicherheitsrichtlinien	Richtlinien zur Passwortsicherheit, zum Umgang mit sensiblen Daten etc.
Notfallplan	Schritte beschreibt, die im Falle eines Sicherheitsvorfalls oder Datenverlusts zu folgen sind
Zugriffskontrollrichtlinien	Zugriffsrechte Verwaltung und Überprüfung, Prozesse für die Vergabe, Änderung und Entfernung von Zugriffsrechten
Bewusstseinsmaterialien	Materialien, die für die Schulung der Mitarbeiter in Bezug auf Sicherheitspraktiken und -bewusstsein verwendet werden

Tabelle 2: Weiterführende Dokumente

* Herausgabe bedarf einer besonderen Erlaubnis

2 Allgemeines

In diesem Abschnitt wird die Methodik zur Erstellung, die gesetzlichen Vorgaben sowie der Geltungsbereich des IT-Sicherheitskonzepts beschrieben. Hier werden alle Punkte erfasst welche die Rahmenbedingungen für dieses Konzept darstellen.

2.1 Methodik

In der Entwicklung unseres IT-Sicherheitskonzepts haben wir uns bewusst für die Anwendung des BSI-Standards entschieden, um eine hohe Qualität und Effektivität unserer Sicherheitsstrategie zu gewährleisten. Der BSI-Standard, entwickelt vom Bundesamt für Sicherheit in der Informationstechnik, ist eine renommierte und weit anerkannte Richtlinie im Bereich der IT-Sicherheit. Dieser Standard bietet einen ganzheitlichen Ansatz, der nicht nur technische, sondern auch organisatorische, personelle und infrastrukturelle Sicherheitsmaßnahmen berücksichtigt. Unsere Entscheidung für diesen Standard basiert auf mehreren Schlüsselüberlegungen:

Ganzheitlicher Sicherheitsansatz: Der BSI-Standard ermöglicht es uns, ein umfassendes Verständnis aller Aspekte der IT-Sicherheit zu entwickeln und umzusetzen. Dies beinhaltet sowohl technische Komponenten als auch organisatorische Strukturen und Prozesse, die für die Aufrechterhaltung einer robusten Sicherheitsumgebung unerlässlich sind.

Einhaltung von Best Practices und Normen: Die Anwendung des BSI-Standards stellt sicher, dass unser Sicherheitskonzept auf bewährten Praktiken und internationalen Normen basiert. Dadurch sind wir in der Lage, sowohl aktuelle als auch zukünftige gesetzliche und regulatorische Anforderungen zu erfüllen und gleichzeitig hohe Sicherheitsstandards aufrechtzuerhalten.

Strukturiertes Risikomanagement: Der BSI-Standard bietet einen systematischen Rahmen für das Risikomanagement. Durch diesen strukturierten Ansatz können wir Sicherheitsrisiken effektiv identifizieren, analysieren und bewerten, um gezielte und angemessene Maßnahmen zu ergreifen.

Anpassbarkeit an Unternehmensbedürfnisse: Der flexible Ansatz des BSI-Standards ermöglicht es uns, das Sicherheitskonzept an die spezifischen Anforderungen und Bedingungen unseres Unternehmens anzupassen. Dies gewährleistet, dass das Konzept sowohl relevant als auch praktikabel in der Anwendung ist.

Fokus auf kontinuierliche Verbesserung: Der BSI-Standard betont die Wichtigkeit der kontinuierlichen Überprüfung und Verbesserung der Sicherheitsmaßnahmen. Dieser Ansatz stimmt mit unserem Ziel überein, stets auf neue Sicherheitsherausforderungen reagieren zu können und unser Sicherheitsniveau kontinuierlich zu erhöhen.

Vertrauensbildung bei Stakeholdern: Durch die Nutzung eines anerkannten Standards wie des BSI-Standards stärken wir das Vertrauen unserer Kunden, Geschäftspartner und Mitarbeiter in unsere Sicherheitsbemühungen.

Allgemeines

Zusammenfassend bietet die Anwendung des BSI-Standards als methodische Grundlage für unser IT-Sicherheitskonzept eine solide Basis, um ein umfassendes, adaptives und proaktives Sicherheitsmanagement zu gewährleisten. Dieser Ansatz unterstützt nicht nur unsere laufenden Sicherheitsbemühungen, sondern stärkt auch unsere Position als verantwortungsbewusstes und zukunftsorientiertes Unternehmen.

2.2 Geltungsbereich und Verantwortlichkeiten

Der Geltungsbereich unseres IT-Sicherheitskonzepts umfasst sämtliche IT-Systeme, Netzwerke, Anwendungen und Daten, die für den Betrieb und die Geschäftsprozesse von **Ships-Without-Diesel-Solution** von Bedeutung sind. Dies schließt sowohl interne Systeme und Infrastrukturen als auch externe Dienste ein, die für das Unternehmen von Bedeutung sind.

Schnittstellen nach Außen

Im Rahmen unseres Verbunds gibt es verschiedene Schnittstellen nach außen, die in diesem Konzept berücksichtigt werden:

Kundenschnittstellen:

Hierbei handelt es sich um Systeme und Prozesse, die für die Interaktion mit Kunden genutzt werden, wie z.B. Kundenportale, Support-Systeme und Kommunikationskanäle.

Lieferanten und Partner:

Dies umfassten alle digitalen Interaktionen und Datenaustauschprozesse mit Lieferanten und Geschäftspartnern.

Remote-Zugriff und mobile Arbeitsplätze:

Hierzu gehören alle Zugriffspunkte, die von außerhalb des Firmennetzwerks genutzt werden, einschließlich VPN-Verbindungen und mobilen Endgeräten.

Verantwortlichkeiten im Verbund

In unserem Verbund sind die Verantwortlichkeiten klar definiert, um eine effektive Sicherheitsstruktur zu gewährleisten:

Technik:

Die Verantwortung für die technischen Aspekte, einschließlich Netzwerkmanagement, Hardware und Software, liegt bei IT-Systemadministrator Sebastian, Breu. Diese Rolle beinhaltet auch die Überwachung der technischen Sicherheitsmaßnahmen und die Reaktion auf technische Sicherheitsvorfälle.

Gebäudemanagement:

Eine Externe Firma ist für die physische Sicherheit unserer Einrichtungen verantwortlich. Dies schließt Zutrittskontrollen, Überwachungssysteme und den Schutz vor physischen Bedrohungen ein.

Datenmanagement und Datenschutz:

Die Verantwortung für den Datenschutz und die Sicherheit der Unternehmensdaten liegt bei IT-Systemadministrator Sebastian Breu. Diese Rolle beinhaltet die Sicherstellung der Datensicherheit, die Einhaltung von Datenschutzvorschriften und die Implementierung von Datenschutzmaßnahmen.

Schnittstellen und Lösungen

Die Schnittstellen werden durch eine Kombination aus technischen und organisatorischen Lösungen gemanagt:

Technische Lösungen beinhalten Firewalls, Verschlüsselung, Zugangskontrollsysteme und Überwachungswerzeuge.

Organisatorische Regelungen umfassen Richtlinien für den Datenaustausch, Verträge mit externen Partnern und Schulungen für Mitarbeiter zur Sensibilisierung für Sicherheitsrisiken. Durch diesen integrierten Ansatz stellen wir sicher, dass sowohl die internen als auch die externen Aspekte unserer IT-Sicherheit effektiv verwaltet werden und dass alle Verantwortlichen klar definierte Rollen und Aufgaben haben.

2.3 Gesetzliche Vorgaben dieses Verfahrens (Compliance)

Unser IT-Sicherheitskonzept beruht auf einer sorgfältigen Analyse und Integration verschiedener gesetzlicher Vorgaben, Normen und unternehmensinterner Richtlinien. Diese Vorgaben bilden das Fundament für unsere Sicherheitsstrategien und -maßnahmen und gewährleisten, dass unser Handeln sowohl rechtlich konform als auch nach Best Practices ausgerichtet ist.

Gesetzliche Grundlagen und Normen:

IT-Grundschutz-Kataloge des BSI (Bundesamt für Sicherheit in der Informationstechnik), Stand 2019: Diese Kataloge bieten umfassende Empfehlungen und Maßnahmen zur Sicherung von IT-Systemen und dienen als Leitfaden für die Entwicklung unseres Sicherheitskonzepts.

BSI-Standards 200-1, 200-2 und 200-3: Diese Standards bilden die Grundlage für unser Informationssicherheits-Managementsystem (ISMS). Der BSI-Standard 200-1 definiert die Anforderungen an ISMS, der BSI-Standard 200-2 gibt die Vorgehensweise für den IT-Grundschutz vor, und der BSI-Standard 200-3 legt die Methodik zur Risikoanalyse fest. Zusätzlich integrieren wir die aktuellen Bausteine des neuen Grundschatzkompendiums in unser Sicherheitsmanagement.

EU-Datenschutz-Grundverordnung (EU-DSGVO): Als rechtliche Grundlage für den Datenschutz ist die EU-DSGVO entscheidend für die Gestaltung unserer Sicherheitsprozesse, insbesondere in Bezug auf die Verarbeitung personenbezogener Daten. Wir stellen sicher, dass alle unsere Prozesse und Systeme in Übereinstimmung mit dieser Verordnung stehen.

Interne Unternehmensvorgaben:

Neben diesen gesetzlichen Vorgaben und Normen orientiert sich unser Sicherheitskonzept auch an internen Richtlinien und Anweisungen der Unternehmensleitung. Diese umfassen:

Unternehmensinterne Sicherheitsrichtlinien: Unsere internen Richtlinien definieren spezifische Sicherheitsstandards und -verfahren, die im gesamten Unternehmen Anwendung finden. Sie umfassen Aspekte wie Zugangskontrollen, Datensicherungsverfahren und Incident-Response-Pläne.

Compliance-Richtlinien: Diese internen Richtlinien stellen sicher, dass unser Unternehmen in Übereinstimmung mit branchenspezifischen Regulierungen und Standards agiert. Sie beinhalten Vorgaben zu Compliance-Prüfungen, Berichterstattung und Verhaltenskodex.

Ethik- und Verhaltenskodex: Unser Unternehmenskodex legt die ethischen Standards und Verhaltenserwartungen an unsere Mitarbeiter fest, insbesondere im Hinblick auf Vertraulichkeit, Integrität und den Umgang mit sensiblen Informationen.

Zusammenfassend basiert unser IT-Sicherheitskonzept auf einer Kombination aus externen gesetzlichen Anforderungen und internen Unternehmensrichtlinien. Diese umfassende Compliance-Struktur stellt sicher, dass unser Unternehmen nicht nur rechtlichen Anforderungen entspricht, sondern auch nach höchsten Sicherheits- und Ethikstandards operiert.

2.4 Personenbezogene Daten

Im Rahmen unseres IT-Sicherheitskonzepts ist der Umgang mit personenbezogenen Daten ein zentraler Aspekt, der besondere Aufmerksamkeit erfordert. Je nach Natur und Umfang unserer Geschäftstätigkeiten kann es vorkommen, dass wir entweder keinen Kontakt mit personenbezogenen Daten haben oder im Gegenteil, in direktem Kontakt mit besonders sensiblen personenbezogenen Daten stehen.

Falls kein Kontakt mit personenbezogenen Daten besteht: In diesem Fall haben unsere Aktivitäten und Prozesse keinen Einfluss auf personenbezogene Daten. Dies bedeutet, dass die Risiken im Zusammenhang mit Datenschutzverletzungen und die Notwendigkeit spezieller Datenschutzmaßnahmen in unserem Kontext gering sind. Dennoch bleiben wir hinsichtlich der allgemeinen Datenschutzpraktiken und -regelungen aufmerksam.

Falls Kontakt mit besonderen personenbezogenen Daten besteht: In diesem Szenario interagieren wir direkt mit sensiblen personenbezogenen Daten, wie Gesundheitsinformationen, biometrischen Daten oder anderen Kategorien, die nach der EU-DSGVO als „besondere Kategorien personenbezogener Daten“ gelten. In diesem Fall gelten strikte Datenschutzmaßnahmen, und es ist entscheidend, dass alle unsere Prozesse und Systeme den höchsten Standards des Datenschutzes entsprechen.

Verweis auf das Datenschutzkonzept

Unabhängig davon, ob wir in direktem Kontakt mit personenbezogenen Daten stehen oder nicht, ist es wichtig, dass alle Mitarbeiter sich der Bedeutung des Datenschutzes bewusst sind und entsprechend handeln. Detaillierte Informationen zur Handhabung personenbezogener Daten, einschließlich der Klassifizierung, Verarbeitung und Sicherung dieser Daten, sind im „Datenschutzkonzept“ unseres Unternehmens festgelegt. Dieses Konzept ist eine wesentliche Anlage zu unserem IT-Sicherheitskonzept und definiert die Richtlinien, Verfahren und Verantwortlichkeiten im Umgang mit personenbezogenen Daten.

Das Datenschutzkonzept beschreibt genau, wie personenbezogene Daten innerhalb unseres Verbunds verwendet, geschützt und verwaltet werden. Es stellt sicher, dass wir nicht nur den rechtlichen Anforderungen entsprechen, sondern auch die Privatsphäre und Sicherheit der betroffenen Personen respektieren und schützen.

3 Strukturanalyse (Ist-Aufnahme)

Die Strukturanalyse kann je nach Ihrem Umfang entweder direkt in Tabellen in dem Dokument des IT-Sicherheitskonzepts erfasst werden. Sie können aber auch, wenn Sie ein Tool für die Erstellung eines IT-Sicherheitskonzepts zurückgreifen, auf den jeweiligen Report verweisen. Sie können auch auf die Übersicht der Struktur in einem anderen Dokument verweisen, wenn sie z.B. die Übersicht über ein Tabellenkalkulationsprogramm dargestellt haben. Oder wenn Sie Software nutzen in welcher alle ihre IT-Objekte erfasst sind steht es ihnen frei auf diese Auszüge zu verweisen.

3.1 Gruppierung

Kürzel	Name																																																												
AP1	WLAN Access Point Produktion																																																												
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>benötigt</td> <td>HP2</td> <td>Switch Produktion</td> </tr> <tr> <td>benötigt</td> <td>N2</td> <td>Firewall Produktion</td> </tr> <tr> <td>benötigt</td> <td>C2/3/6/7<>AP1</td> <td>Client Produktion<>WLAN AP Produktion</td> </tr> <tr> <td>benötigt</td> <td>K44</td> <td>Kaffeemaschine <> WLAN AP PROD</td> </tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	benötigt	HP2	Switch Produktion	benötigt	N2	Firewall Produktion	benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion	benötigt	K44	Kaffeemaschine <> WLAN AP PROD	Administrator	Admin	Sebastian Breu																																										
Zuordnung	Kürzel	Name																																																											
benötigt	HP2	Switch Produktion																																																											
benötigt	N2	Firewall Produktion																																																											
benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion																																																											
benötigt	K44	Kaffeemaschine <> WLAN AP PROD																																																											
Administrator	Admin	Sebastian Breu																																																											
AP2	WLAN Access Point Betrieb																																																												
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>benötigt</td> <td>HP1</td> <td>Switch Betrieb</td> </tr> <tr> <td>benötigt</td> <td>N1</td> <td>Firewall Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C1/4/5<>AP2</td> <td>Client Betrieb<>WLAN AP Betrieb</td> </tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	benötigt	HP1	Switch Betrieb	benötigt	N1	Firewall Betrieb	benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb	Administrator	Admin	Sebastian Breu																																													
Zuordnung	Kürzel	Name																																																											
benötigt	HP1	Switch Betrieb																																																											
benötigt	N1	Firewall Betrieb																																																											
benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb																																																											
Administrator	Admin	Sebastian Breu																																																											
C1	Client Betrieb Laptop																																																												
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP02</td> <td>Einkauf</td> </tr> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td> </tr> <tr> <td>nötig für</td> <td>GP05</td> <td>Technischer Support</td> </tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td> </tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td> </tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td> </tr> <tr> <td>nötig für</td> <td>A05</td> <td>Word</td> </tr> <tr> <td>benötigt</td> <td>C1/4/5<>AP2</td> <td>Client Betrieb<>WLAN AP Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C1/4/5<>N1</td> <td>Client Betrieb<>Firewall Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C1<>C2</td> <td>Client Betrieb<>Client Produktion</td> </tr> <tr> <td>benötigt</td> <td>C1<>C4</td> <td>Client Betrieb<>Client Sekretär</td> </tr> <tr> <td>benötigt</td> <td>C1<>C5</td> <td>Client Betrieb<>Client Geschäftsführung</td> </tr> <tr> <td>benötigt</td> <td>C1<>D1</td> <td>Client Betrieb<>Drucker Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C1<>S1</td> <td>Client Betrieb<>Server Betrieb</td> </tr> <tr> <td>benötigt</td> <td>C4<>C5</td> <td>Client Sekretär<>Client Geschäftsführung</td> </tr> <tr> <td>benötigt</td> <td>HP1<>C1/4/5</td> <td>Switch Betrieb<>Client Betrieb</td> </tr> <tr> <td>Anwender</td> <td></td> <td>Ulrike Schmidt</td> </tr> <tr> <td>Verantwortlicher</td> <td></td> <td>Heinrich Henckel von Donnersmarck</td> </tr> <tr> <td>Administrator</td> <td>Admin</td> <td>Sebastian Breu</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP02	Einkauf	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	GP05	Technischer Support	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A04	TeamViewer	nötig für	A05	Word	benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb	benötigt	C1/4/5<>N1	Client Betrieb<>Firewall Betrieb	benötigt	C1<>C2	Client Betrieb<>Client Produktion	benötigt	C1<>C4	Client Betrieb<>Client Sekretär	benötigt	C1<>C5	Client Betrieb<>Client Geschäftsführung	benötigt	C1<>D1	Client Betrieb<>Drucker Betrieb	benötigt	C1<>S1	Client Betrieb<>Server Betrieb	benötigt	C4<>C5	Client Sekretär<>Client Geschäftsführung	benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb	Anwender		Ulrike Schmidt	Verantwortlicher		Heinrich Henckel von Donnersmarck	Administrator	Admin	Sebastian Breu
Zuordnung	Kürzel	Name																																																											
nötig für	GP02	Einkauf																																																											
nötig für	GP03	Auftragsannahme / Verkauf																																																											
nötig für	GP05	Technischer Support																																																											
nötig für	A01	Excel																																																											
nötig für	A02	Outlook																																																											
nötig für	A04	TeamViewer																																																											
nötig für	A05	Word																																																											
benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb																																																											
benötigt	C1/4/5<>N1	Client Betrieb<>Firewall Betrieb																																																											
benötigt	C1<>C2	Client Betrieb<>Client Produktion																																																											
benötigt	C1<>C4	Client Betrieb<>Client Sekretär																																																											
benötigt	C1<>C5	Client Betrieb<>Client Geschäftsführung																																																											
benötigt	C1<>D1	Client Betrieb<>Drucker Betrieb																																																											
benötigt	C1<>S1	Client Betrieb<>Server Betrieb																																																											
benötigt	C4<>C5	Client Sekretär<>Client Geschäftsführung																																																											
benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb																																																											
Anwender		Ulrike Schmidt																																																											
Verantwortlicher		Heinrich Henckel von Donnersmarck																																																											
Administrator	Admin	Sebastian Breu																																																											
C1	Client Betrieb APC																																																												
	<table> <thead> <tr> <th>Zuordnung</th> <th>Kürzel</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>nötig für</td> <td>GP02</td> <td>Einkauf</td> </tr> <tr> <td>nötig für</td> <td>GP03</td> <td>Auftragsannahme / Verkauf</td> </tr> <tr> <td>nötig für</td> <td>GP05</td> <td>Technischer Support</td> </tr> <tr> <td>nötig für</td> <td>A01</td> <td>Excel</td> </tr> <tr> <td>nötig für</td> <td>A02</td> <td>Outlook</td> </tr> <tr> <td>nötig für</td> <td>A04</td> <td>TeamViewer</td> </tr> </tbody> </table>	Zuordnung	Kürzel	Name	nötig für	GP02	Einkauf	nötig für	GP03	Auftragsannahme / Verkauf	nötig für	GP05	Technischer Support	nötig für	A01	Excel	nötig für	A02	Outlook	nötig für	A04	TeamViewer																																							
Zuordnung	Kürzel	Name																																																											
nötig für	GP02	Einkauf																																																											
nötig für	GP03	Auftragsannahme / Verkauf																																																											
nötig für	GP05	Technischer Support																																																											
nötig für	A01	Excel																																																											
nötig für	A02	Outlook																																																											
nötig für	A04	TeamViewer																																																											

Strukturanalyse (Ist-Aufnahme)

Kürzel	Name	
nötig für	A05	
benötigt	C1/4/5<>AP2	
benötigt	C1/4/5<>N1	
benötigt	C1<>C2	
benötigt	C1<>C4	
benötigt	C1<>C5	
benötigt	C1<>D1	
benötigt	C1<>S1	
benötigt	C4<>C5	
benötigt	HP1<>C1/4/5	
Anwender	Doris Richarz	
Verantwortlicher	Lieselotte Hans	
Administrator	Admin	
C2	Client Produktion	
Zuordnung	Kürzel	Name
nötig für	GP01	Konstruktion
nötig für	GP04	Fertigung
nötig für	A01	Excel
nötig für	A02	Outlook
nötig für	A03	Delftship
nötig für	A04	TeamViewer
benötigt	D2	Drucker Produktion
benötigt	C1<>C2	Client Betrieb<>Client Produktion
benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion
benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme
benötigt	C2/C3/C6/C7<>N2	Client Produktion<>Firewall Produktion
benötigt	C2<>C3	Client Produktion<>Client Produktionsleiter
benötigt	C2<>C6	Client Produktion<>Client CNC Fräse
benötigt	C2<>C7	Client Produktion<>Client Gussmaschine
benötigt	C2<>D2	Client Produktion<>Drucker Produktion
benötigt	C2<>S2	Client Produktion<>Server Produktion
benötigt	HP2<>C2/3	Switch Produktion<>Client Produktion
Anwender	Nicolas Traidl	
Verantwortlicher	Mia Lindenberg	
Administrator	Admin	
C3	Client Produktionsleiter	
Zuordnung	Kürzel	Name
nötig für	GP01	Konstruktion
nötig für	GP04	Fertigung
nötig für	A01	Excel
nötig für	A02	Outlook
nötig für	A03	Delftship
nötig für	A04	TeamViewer
benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion
benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme
benötigt	C2/C3/C6/C7<>N2	Client Produktion<>Firewall Produktion
benötigt	C2<>C3	Client Produktion<>Client Produktionsleiter
benötigt	C2<>S2	Client Produktion<>Server Produktion
benötigt	C3<>D2	Client Produktionsleiter<>Drucker Produktion
benötigt	HP2<>C2/3	Switch Produktion<>Client Produktion
Verantwortlicher	Mia Lindenberg	
Administrator	Admin	
C4	Client Sekretär	
Zuordnung	Kürzel	Name
nötig für	GP03	Auftragsannahme / Verkauf
nötig für	A01	Excel
nötig für	A02	Outlook

Strukturanalyse (Ist-Aufnahme)

Kürzel	Name	
nötig für	A04	
nötig für	A05	
benötigt	C1/4/5<>AP2	
benötigt	C1/4/5<>N1	
benötigt	C1<>C4	
benötigt	C1<>S1	
benötigt	C4<>D1	
benötigt	HP1<>C1/4/5	
Administrator	Admin	
Anwender	Sekretär	
Verantwortlicher	Sekretär	
C5 Client Geschäftsführung		
Zuordnung	Kürzel	Name
nötig für	A01	Excel
nötig für	A02	Outlook
nötig für	A04	TeamViewer
nötig für	A05	Word
VM-Host für	C5	Client Geschäftsführung
benötigt	C1/4/5<>AP2	Client Betrieb<>WLAN AP Betrieb
benötigt	C1/4/5<>N1	Client Betrieb<>Firewall Betrieb
benötigt	C1<>C5	Client Betrieb<>Client Geschäftsführung
benötigt	C1<>S1	Client Betrieb<>Server Betrieb
benötigt	C4<>C5	Client Sekretär<>Client Geschäftsführung
benötigt	C5<>D1	Client Geschäftsführung<>Drucker Betrieb
benötigt	HP1<>C1/4/5	Switch Betrieb<>Client Betrieb
befindet sich in	EG-1	Büro Raum Geschäftsführer
Administrator	Admin	Sebastian Breu
Anwender	CEO	Ulrich Meissen
Verantwortlicher	CEO	Ulrich Meissen
C6 Client CNC Fräse		
Zuordnung	Kürzel	Name
nötig für	GP04	Fertigung
nötig für	A01	Excel
nötig für	A02	Outlook
nötig für	A03	Delftship
nötig für	A04	TeamViewer
benötigt	S101	Produktionsmaschine - CNC Fräse
benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion
benötigt	C2<>C6	Client Produktion<>Client CNC Fräse
benötigt	C2<>C7	Client Produktion<>Client Gussmaschine
benötigt	C2<>S2	Client Produktion<>Server Produktion
Verantwortlicher		Sylvia Gradl
Administrator	Admin	Sebastian Breu
C7 Client Gussmaschine		
Zuordnung	Kürzel	Name
nötig für	GP04	Fertigung
nötig für	A01	Excel
nötig für	A02	Outlook
nötig für	A03	Delftship
nötig für	A04	TeamViewer
benötigt	S102	Produktionsmaschine - Gussmaschine
benötigt	C2/3/6/7<>AP1	Client Produktion<>WLAN AP Produktion
benötigt	C2<>S2	Client Produktion<>Server Produktion
Administrator	Admin	Sebastian Breu
D1 Drucker Betrieb		
Zuordnung	Kürzel	Name
nötig für	GP02	Einkauf
nötig für	GP03	Auftragsannahme / Verkauf
benötigt	N1	Firewall Betrieb
nötig für	S1	Server Betrieb

Strukturanalyse (Ist-Aufnahme)

Kürzel	Name		
benötigt	C1<>D1	Client Betrieb	<>Drucker Betrieb
benötigt	C4<>D1	Client Sekräter	<>Drucker Betrieb
benötigt	C5<>D1	Client Geschäftsführung	<>Drucker Betrieb
Anwender		Ulrike Schmidt	
Verantwortlicher	Admin	Sebastian Breu	
Anwender	HR	Michael Holzhüter	
D2	Drucker Produktion		
Zuordnung	Kürzel	Name	
nötig für	C2	Client Produktion	
benötigt	N2	Firewall Produktion	
benötigt	S2	Server Produktion	
benötigt	C2<>D2	Client Produktion	<>Drucker Produktion
benötigt	C3<>D2	Client Produktionsleiter	<>Drucker Produktion
Anwender		Nicolas Traidl	
Verantwortlicher	Admin	Sebastian Breu	
HP1	Switch Betrieb		
Zuordnung	Kürzel	Name	
nötig für	AP2	WLAN Access Point Betrieb	
benötigt	N1	Firewall Betrieb	
nötig für	S1	Server Betrieb	
benötigt	HP1<>C1/4/5	Switch Betrieb	<>Client Betrieb
HP2	Switch Produktion		
Zuordnung	Kürzel	Name	
nötig für	AP1	WLAN Access Point Produktion	
benötigt	N2	Firewall Produktion	
nötig für	S2	Server Produktion	
benötigt	HP2<>C2/3	Switch Produktion	<>Client Produktion
N1	Firewall Betrieb		
Zuordnung	Kürzel	Name	
nötig für	GP02	Einkauf	
nötig für	GP03	Auftragsannahme / Verkauf	
nötig für	GP05	Technischer Support	
nötig für	AP2	WLAN Access Point Betrieb	
nötig für	D1	Drucker Betrieb	
nötig für	HP1	Switch Betrieb	
benötigt	R1	Router	
nötig für	S1	Server Betrieb	
benötigt	C1/4/5<>N1	Client Betrieb	<>Firewall Betrieb
benötigt	K43	Router	<>Internet
benötigt	K45	Firewall Betrieb	<->Router
benötigt	K46	Firewall Betrieb	<>Firewall Produktion
benötigt	S1<>N1	Server Betrieb	<>Firewall Betrieb
befindet sich in	OG-5	Serverraum	
Administrator	Admin	Sebastian Breu	
N2	Firewall Produktion		
Zuordnung	Kürzel	Name	
nötig für	GP01	Konstruktion	
nötig für	GP04	Fertigung	
nötig für	AP1	WLAN Access Point Produktion	
nötig für	D2	Drucker Produktion	
nötig für	HP2	Switch Produktion	
benötigt	R1	Router	
virtualisiert auf	S2	Server Produktion	
benötigt	C2/C3/C6/C7<>N2	Client Produktion	<>Firewall Produktion
benötigt	K40	Firewall Prod	<> Router
benötigt	K43	Router	<>Internet
benötigt	K46	Firewall Betrieb	<>Firewall Produktion
benötigt	S2<>N2	Server Produktion	<>Firewall Produktion
befindet sich in	OG-5	Serverraum	
Administrator	Admin	Sebastian Breu	

Strukturanalyse (Ist-Aufnahme)

Kürzel	Name		
R1	Router		
	Zuordnung	Kürzel	Name
	nötig für	GP01	Konstruktion
	nötig für	GP02	Einkauf
	nötig für	GP03	Auftragsannahme / Verkauf
	nötig für	GP04	Fertigung
	nötig für	GP05	Technischer Support
	nötig für	N1	Firewall Betrieb
	nötig für	N2	Firewall Produktion
	benötigt	K40	Firewall Prod <> Router
	benötigt	K42	Router<>Videoüberwachung
	benötigt	K43	Router<>Internet
	benötigt	K45	Firewall Betrieb<->Router
	befindet sich in	OG-5	Serverraum
	Administrator	Admin	Sebastian Breu
S1	Server Betrieb		
	Zuordnung	Kürzel	Name
	nötig für	GP02	Einkauf
	nötig für	GP03	Auftragsannahme / Verkauf
	nötig für	GP05	Technischer Support
	nötig für	A01	Excel
	nötig für	A02	Outlook
	nötig für	A04	TeamViewer
	nötig für	A05	Word
	benötigt	D1	Drucker Betrieb
	benötigt	HP1	Switch Betrieb
	benötigt	N1	Firewall Betrieb
	benötigt	C1<>S1	Client Betrieb<>Server Betrieb
	benötigt	S1<>N1	Server Betrieb<>Firewall Betrieb
	benötigt	S1<>S2	Server Betrieb<>Server Produktion
	befindet sich in	OG-5	Serverraum
	Administrator	Admin	Sebastian Breu
S2	Server Produktion		
	Zuordnung	Kürzel	Name
	nötig für	GP01	Konstruktion
	nötig für	GP04	Fertigung
	nötig für	A01	Excel
	nötig für	A02	Outlook
	nötig für	A03	Delftship
	nötig für	A04	TeamViewer
	nötig für	D2	Drucker Produktion
	benötigt	HP2	Switch Produktion
	VM-Host für	N2	Firewall Produktion
	benötigt	C2<>S2	Client Produktion<>Server Produktion
	benötigt	S1<>S2	Server Betrieb<>Server Produktion
	benötigt	S2<>N2	Server Produktion<>Firewall Produktion
	befindet sich in		Halle und Materiallager
	Administrator	Admin	Sebastian Breu

ICS-System

Kürzel	Name		
S101	Produktionsmaschine - CNC Fräse		
	Zuordnung	Kürzel	Name
	nötig für	GP04	Fertigung
	nötig für	C6	Client CNC Fräse
	benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme
	befindet sich in		Halle und Materiallager
	Verantwortlicher		Sylvia Gradl

Strukturanalyse (Ist-Aufnahme)

Kürzel Name			
S102	Produktionsmaschine Gussmaschine	-	
Zuordnung	Kürzel	Name	
nötig für	GP04	Fertigung	
nötig für	C7	Client Gussmaschine	
benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme	
befindet sich in		Halle und Materiallager	
Verantwortlicher		Sylvia Gradl	
S100	SPS		
Zuordnung	Kürzel	Name	
nötig für	GP04	Fertigung	
benötigt	C2/3<>S100/S101/102	Client Produktion/Produktionsleiter<>ICS-Systeme	
befindet sich in		Halle und Materiallager	
Verantwortlicher		Sylvia Gradl	

Anderes/IoT-System

Kürzel Name			
I1	Videoüberwachung		
Zuordnung	Kürzel	Name	
benötigt	K42	Router<>Videoüberwachung	
K1	Kaffeemaschine		
Zuordnung	Kürzel	Name	
benötigt	K44	Kaffeemaschine <> WLAN AP PROD	
befindet sich in	EG-6	Küche	

3.2 Relevante Geschäftsprozesse und dazugehörige Informationen

Fügen Sie hier die passende Tabelle zu Ihren Geschäftsprozessen ein oder Verweisen auf den jeweiligen Auszug eines Tools. Bei den Geschäftsfällen müssen die Kern- und Unterstützenden Prozesse ersichtlich werden. Achten Sie bei den Geschäftsfällen auf einen passenden Granularitätsgrad.

Siehe Dokument:

[ITKS_A.1_Strukturanalyse-Abhängigkeiten_Informationsverbund_2024-01-23.pdf](#)

3.3 Relevante Anwendungen und dazugehörige Informationen

Beschreiben Sie nun nach dem Beispiel der Geschäftsfälle auch die Anwendungen welche im Verbund vorhanden sind. Hierbei ist es nicht notwendig das jede der Anwendungen auch einen Geschäftsfall zuzuordnen ist. Wichtig ist das keine der genutzten Anwendungen vergessen wird. Zur Übersichtlichkeit empfiehlt es sich nur die wichtigsten Informationen im Konzept niederzuschreiben. Vollständig können Sie die Informationen in Anlagen hinterlegen. Entweder durch die Übersicht der Reports aus unterstützenden Tools.

Strukturanalyse (Ist-Aufnahme)

Anwendungen

Kürzel	Name	Beschreibung	Plattform / Baustein	Anzahl	Status
A01	Excel	Excel ermöglicht es den Mitarbeitern, umfangreiche Datenmengen aus Produktion und Vertrieb zu verarbeiten, zu analysieren und zu präsentieren. Excel wird für die Erstellung von Produktionsplänen, Verkaufsprognosen und Budgets genutzt.	MS Windows/APP.1.1	29	Betrieb
	Benutzer:	Produktion, Vertrieb			
A02	Outlook	Outlook ermöglicht es den Mitarbeitern, E-Mails zu senden und zu empfangen, wodurch die interne und externe Kommunikation erleichtert wird.	MS Windows/APP.5.2	29	Betrieb

Tabelle 3: Anwendungen

Restliche Dokumentation siehe Dokument:

[ITKS_A.1_Strukturanalyse-Abhängigkeiten_Informationsverbund_2024-01-23.pdf](#)

3.3.1 Zuordnung Geschäftsprozesse zu Anwendungen

Siehe Dokument:

[ITKS_A.1_Strukturanalyse-Abhängigkeiten_Informationsverbund_2024-01-23.pdf](#)

3.3.2 Technologieübersicht der einzelnen Anwendungen

Siehe Dokument:

[ITKS_A.1_Strukturanalyse-Abhängigkeiten_Informationsverbund_2024-01-23.pdf](#)

3.4 Netzplan

Der Netzwerkplan enthält eine Vielzahl von wichtigen Informationen für die Strukturanalyse deshalb sollte dieser hier erwähnt und wenn möglich eingefügt werden. Es bietet sich an Informationen zum Verständnis des Netzwerkplans zu notieren.

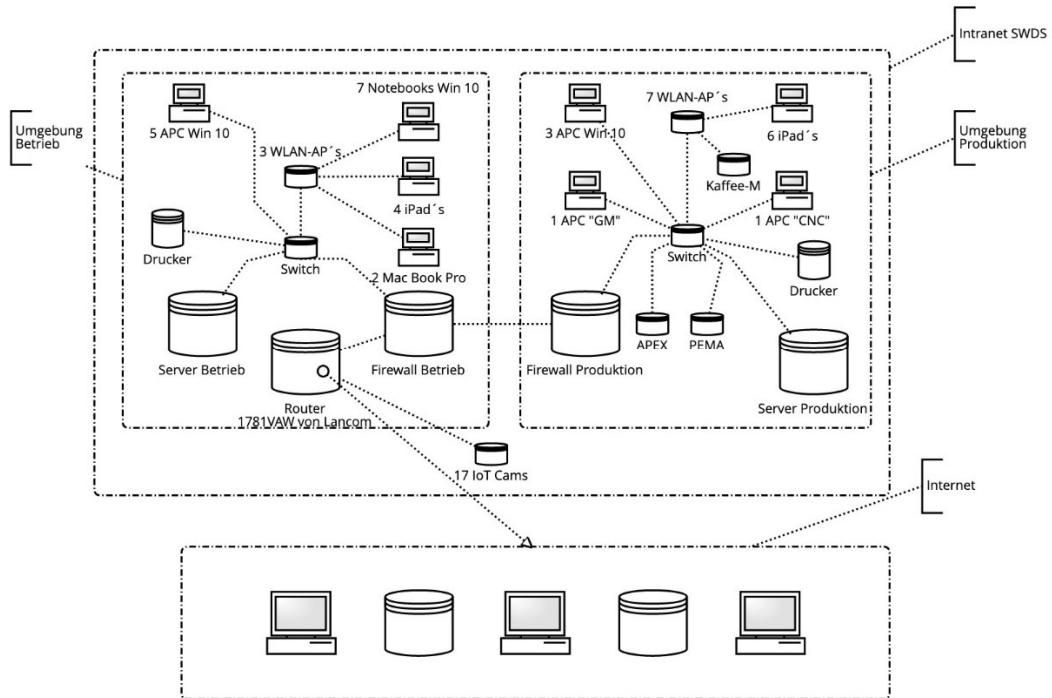


Abbildung 1: Netzplan

3.1 IT-Systeme, ICS-Systeme, IoT-Geräte

Wie schon bei dem Schema der Geschäftsfälle und Anwendungen werden nun die IT Systeme, ICS Systeme und IoT Geräte erfasst und aufgelistet. Alle wesentlichen Informationen wie die Anzahl der Systeme, Anwender und Verantwortliche sollten erfasst sein. Eine zusätzliche Beschreibung der Inhalte der Tabelle ist optional.

Siehe Dokument:

[ITKS_A.1_Strukturanalyse-Abhängigkeiten_Informationsverbund_2024-01-23.pdf](#)

[ITKS_A.1_Strukturanalyse_Informationsverbund_2024-01-23.pdf](#)

Auch die IT-Systeme, ICS-Systeme und IoT Geräte sollten mit den jeweiligen Anwendungen in Kontext gebracht werden, welche Sie in der Ausführung unterstützen.

Siehe Dokument:

[ITKS_A.1_Strukturanalyse-Abhängigkeiten_Informationsverbund_2024-01-23.pdf](#)

3.2 Kommunikationspfade

Die im Netzwerkplan aufgeführten Verbindungen sollten zum besseren Verständnis gesondert betrachtet und beschrieben werden. Evtl. ergeben sich aus den Geschäftsfällen auch Kommunikationsprozesse dann kann es sich anbieten diesen Ablauf genauer zu beschreiben. Vor allem bei einem IT-Sicherheitskonzept für Produkte müssen den Kommunikationsprozesse gesondert betrachtet werden.

[ITKS_A.1_Strukturanalyse-Abhängigkeiten_Informationsverbund_2024-01-23.pdf](#)

3.3 Betrachtung der Räume

Die Räume und Gebäude werden ebenfalls nach dem Schema der Geschäftsfälle, Anwendungen und Systeme erfasst. Auch hierbei kann eine Gruppenbildung von Vorteil sein. Sollten Besonderheiten wie z.B. Zugangsbeschränkungen in bestimmten Bereichen gelten so sind diese mit aufzuführen.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
	Halle und Materiallager		M Sehr Hoch	M Sehr Hoch	M Sehr Hoch
EG-1	Büro Raum Geschäftschef		Hoch Das Büro des Geschäftschefs enthält vertrauliche Geschäftsinformationen, wie strategische Pläne, finanzielle Daten, Verträge und personenbezogene Informationen. Der Schutz dieser Informationen ist entscheidend, um unautorisierten Zugriff und potenzielle Datenschutzverletzungen zu verhindern.	Hoch Die Integrität der Informationen im Büro des Geschäftschefs ist von grundlegender Bedeutung, um sicherzustellen, dass keine unbefugten Änderungen oder Manipulationen an strategischen Dokumenten, Verträgen und anderen geschäftskritischen Unterlagen vorgenommen werden.	Hoch Die Verfügbarkeit der Informationen im Büro des Geschäftschefs ist entscheidend für effektive Entscheidungsfindung und Geschäftsführung.
EG-2	Büro Raum Personal		Sehr Hoch Der Büro Raum für HR enthält hochsensible personenbezogene Daten, wie Mitarbeiterverträge, Gehaltsinformationen, Leistungsbeurteilungen und möglicherweise auch Informationen zu Mitarbeitergesundheit und -qualifikationen.	Hoch Die Integrität der HR-Daten ist entscheidend, um sicherzustellen, dass die Informationen genau, konsistent und vollständig sind.	Hoch Die Verfügbarkeit von HR-Informationen ist wichtig, um eine effiziente Personalarbeit zu gewährleisten.
EG-3	Büro Raum Entwicklung		Hoch Der Büro Raum enthält hochsensible Konstruktionspläne und technische Zeichnungen für Schiffe. Diese Pläne können geistiges Eigentum,	Hoch Die Integrität der Schiffspläne ist von höchster Wichtigkeit, um sicherzustellen, dass die Konstruktionsinformationen korrekt	Hoch Die Verfügbarkeit der Schiffspläne ist für den reibungslosen Fortschritt der Entwicklungswelt entscheidend. Der Büro Raum sollte so gestaltet

Strukturanalyse (Ist-Aufnahme)

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
			Patente und fortgeschrittene technische Informationen enthalten, die von strategischer Bedeutung für das Unternehmen sind.	und unverändert bleiben.	sein, dass Entwickler jederzeit Zugriff auf ihre Arbeitsunterlagen haben, um effizient und zeitnah arbeiten zu können.
EG-4	Büro Raum Einkauf		Hoch Der Büro Raum enthält vertrauliche Informationen über Schiffsdetails und Einkaufsaktivitäten, darunter möglicherweise Preisverhandlungen, Lieferantenverträge und andere geschäftskritische Informationen.	Hoch Die Integrität der Informationen im Zusammenhang mit Schiffsdetails und Teilebeschaffung ist von entscheidender Bedeutung, um sicherzustellen, dass die beschafften Produkte den erforderlichen Standards entsprechen und keine Risiken für die Schiffskonstruktion darstellen.	Hoch Die Verfügbarkeit von Schiffsdetails und Teileinformationen ist entscheidend für den reibungslosen Ablauf der Beschaffungsaktivitäten. Der Büro Raum sollte so gestaltet sein, dass das Einkaufsteam jederzeit auf die benötigten Unterlagen zugreifen kann, um effiziente und zeitnahe Entscheidungen zu treffen.
EG-5	Empfang/Wartebereich	M	Unbearbeitet	M Unbearbeitet	M Unbearbeitet
EG-6	Küche	M	Unkritisch	M Unkritisch	M Unkritisch
LG-1	Büro Raum Produktion		Hoch Das Büro enthält vertrauliche Informationen über Produktionspläne, Technologien, Konstruktionszeichnungen und möglicherweise auch Informationen zu Materialbeschaffung und Herstellungsprozessen.	Hoch Die Integrität von Produktionsplänen und Konstruktionszeichnungen ist unerlässlich, um sicherzustellen, dass die hergestellten oder reparierten Schiffe den erforderlichen Standards entsprechen.	Hoch Die Verfügbarkeit ist entscheidend für einen effizienten Ablauf der Schiffsbau- und Reparaturprozesse. Das Büro sollte so gestaltet sein, dass die Produktionsmitarbeiter jederzeit auf die benötigten Informationen zugreifen können, um den Bau oder die Reparatur von

Strukturanalyse (Ist-Aufnahme)

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit		Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
			M	U		
LG-2	Küche		M	Unbearbeitet	M	Unbearbeitet
OG-1	Büro Raum Vertrieb		Hoch	Der Büror Raum enthält hochvertrauliche Kundendaten, einschließlich persönlicher Informationen, Verträge, Bestellungen und finanzieller Angaben. Die Vertraulichkeit ist von höchster Bedeutung, um den Schutz der Kunden und die Einhaltung datenschutzrechtlicher Bestimmungen sicherzustellen.	Hoch Die Integrität von Kundenaufträgen und -daten ist entscheidend, um sicherzustellen, dass Transaktionen genau und zuverlässig abgewickelt werden.	Hoch Die Verfügbarkeit von Kundenaufträgen und -daten ist entscheidend für die reibungslose Abwicklung von Verkaufsaktivitäten und Kundenservice. Der Büror Raum sollte so gestaltet sein, dass das Vertriebsteam jederzeit auf die benötigten Informationen zugreifen kann, um Kundenanfragen zu bearbeiten und Bestellungen effizient zu verwalten.
OG-2	Büro Raum IT Admin		Hoch	Das Büro des IT-Administrators enthält vertrauliche Informationen über Sicherheitsrichtlinien, Zugangsberechtigungen und Passwörter.	Hoch Die Integrität von IT-Konfigurationen und -Daten ist unerlässlich, um sicherzustellen, dass das Netzwerk stabil und sicher bleibt.	Hoch Die Verfügbarkeit des IT-Administrators ist entscheidend für den reibungslosen Betrieb der IT-Infrastruktur. Das Büro sollte so gestaltet sein, dass der Administrator jederzeit auf notwendige Tools, Dokumentationen und Ressourcen zugreifen kann, um Probleme schnell zu identifizieren und zu lösen.
OG-3	Büro Raum CISO		Hoch	Das Büro des IT-Sicherheitsbeauftragten enthält hochvertrauliche Informationen über	Hoch Die Integrität von Sicherheitsrichtlinien, Berichten und Analysen ist wesentlich, um	Hoch Die Verfügbarkeit des IT-Sicherheitsbeauftragten ist entscheidend für

Strukturanalyse (Ist-Aufnahme)

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
			Sicherheitsrichtlinien, Schwachstellenanalysen, Incident-Response-Pläne und andere sensible Sicherheitsdokumentationen.	sicherzustellen, dass die Sicherheitsstrategie konsistent und effektiv bleibt.	eine schnelle Reaktion auf Sicherheitsvorfälle und die laufende Überwachung der Sicherheitslage. Das Büro sollte so gestaltet sein, dass der Sicherheitsbeauftragte jederzeit auf notwendige Ressourcen, Berichte und Sicherheitswerkzeuge zugreifen kann.
OG-4	Pausenraum		M Unbearbeitet	M Unbearbeitet	M Unbearbeitet
OG-5	Serverraum		M Sehr Hoch	M Sehr Hoch	M Sehr Hoch

Tabelle 4: Räume

4 Schutzbedarfsfeststellung

Ziel dieser Schutzbedarfsfeststellung ist es, festzustellen, welchen Schutzbedarf die in der Strukturanalyse erfassten Objekte bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Die Bewertungsgrundlage dieses Schutzbedarfs orientiert sich an den potentiellen Beeinträchtigungen, die aufgrund eines Schadens der betroffenen Anwendungen und Geschäftsprozesse entstehen.

4.1 Definition der Schutzbedarfskategorien

Zunächst werden die Schutzbedarfskategorien definiert, indem die Schutzziele sowie die Schadenskategorien für die nachstehenden Betrachtungen bestimmt werden. Zur Abgrenzung der Schutzbedarfskategorien werden anschließend noch einzelne Schadensszenarien und deren Grenzen bestimmt. Anschließend werden die Schutzziele und individualisierten Kategorien auf die Bestandteile des IT-Verbundes angewendet.

4.1.1 Schutzziele

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten (Informationen) und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben bzgl. der Erstellung manipuliert wurden.

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets, wie vorgesehen, genutzt werden können.

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

4.1.2 Schadenskategorien

Der Schutzbedarf der Geschäftsprozesse und Anwendungen ist normal, wenn die Schadensauswirkungen begrenzt und überschaubar sind.

Sind die Schadensauswirkungen beträchtlich, ist der Schutzbedarf hoch.

Geschäftsprozesse und Anwendungen haben einen sehr hohen Schutzbedarf, wenn die Schadensauswirkungen ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

4.1.3 Individualisierte Schutzbedarfskategorien

Die folgende Tabelle beinhaltet die, für die Institution angepassten, Definitionen der Schadenskategorien als Beispiel. Es können weitere Schadenskategorien hinzugezogen werden oder evtl. entfernt werden, wenn diese nicht betrachtet werden müssen in Ihrem Verbund.

Beeinträchtigungs-kategorien	Verlust von	Bedrohung	Schutzbedarf feststellung Kategorien		
			normal	hoch	sehr hoch
1. Beeinträchtigung der Aufgabenerfüllung	Vertraulichkeit	Die unbefugte Preisgabe von Daten	...würde die Aufgabenerfüllung nur geringfügig beeinträchtigen bzw. verzögern.	...behindert die Aufgabenerfüllung ...schränkt die Aufgabenerfüllung in einem Teilbereich ein – tolerierbare Ausfallzeit zwischen einer und 24 Stunden	...würde die Aufgabenerfüllung unmöglich machen. ...gefährdet den Gesamtauftrag der Betroffenen – tolerierbare Ausfallzeit weniger als eine Stunde.
	Integrität	Die Manipulation der Daten bzw. der Funktionsweise	...führt maximal zum Ausfall einzelner Arbeitsabläufe – tolerierbare Ausfallzeit ist größer als 24 Stunden.		
	Verfügbarkeit	Ein Ausfall des Systems, diverser Funktionen oder Anwendungen			
2. Negative Innen- und Außenwirkung	Vertraulichkeit	Die unbefugte Preisgabe von Daten	...führt zu einem geringfügigen Ansehens- und Vertrauensverlust in einer eingeschränkten Öffentlichkeit.	...führt zu einem Ansehens- und Vertrauensverlust bei einer eingeschränkten Öffentlichkeit.	...führt zu einem umfassenden Vertrauensverlust in einer breiten Öffentlichkeit.
	Integrität	Die Manipulation der Daten bzw. der Funktionsweise			
	Verfügbarkeit	Ein Ausfall des Systems, diverser			

Schutzbedarfsfeststellung

Beeinträchtigungs-kategorien	Verlust von	Bedrohung	Schutzbedarfsfeststellung Kategorien		
			normal	hoch	sehr hoch
		Funktionen oder Anwendungen			
3. Finanzielle Auswirkungen	Vertraulichkeit	Die unbefugte Preisgabe von Daten	...führt zu finanziellen Schäden bis 5.000 €.	...führt zu finanziellen Schäden von 5001 bis 50.000 €.	...führt zu finanziellen Schäden größer 50.000 €.
	Integrität	Die Manipulation der Daten bzw. der Funktionsweise			
	Verfügbarkeit	Ein Ausfall des Systems, diverser Funktionen oder Anwendungen			
4. Beeinträchtigung des Informationellen Selbstbestimmungsrechts (Datenschutz)	Vertraulichkeit	Die unbefugte Preisgabe von (pbz.) Daten	...hat geringfügige Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse Betroffener. ...greift nur geringfügig in das informationelle Selbstbestim-	...hat Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse Betroffener. ...greift erheblich in das informationelle Selbstbestimmungsrecht der Betroffenen ein, was	..hat ruinöse Auswirkungen auf die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse Betroffener. ...greift intensiv in das informationelle
	Integrität	Die Manipulation der (pbz.) Daten bzw. der Funktionsweise			
	Verfügbarkeit	Ein Ausfall des Systems, diverser Funktionen oder Anwendungen und dem damit			

Schutzbedarfsfeststellung

Beeinträchtigungs-kategorien	Verlust von	Bedrohung	Schutzbedarfsfeststellung Kategorien		
			normal	hoch	sehr hoch
			fehlenden Zugriff auf (pbz.) Daten	mungsrecht der Betroffenen ein.	durch den Einzelnen toleriert wird.
5. Beeinträchtigung der persönlichen Unversehrtheit	Vertraulichkeit	Die unbefugte Preisgabe von Daten	...lassen eine Beeinträchtigung der persönlichen Unversehrtheit nicht möglich erscheinen.	...lassen eine Beeinträchtigung der persönlichen Unversehrtheit nicht ganz ausgeschlossen erscheinen.	...ermöglichen eine gravierende Beeinträchtigung der der persönlichen Unversehrtheit. ...stellt eine Gefahr für Leib oder Leben dar.
	Integrität	Die Manipulation der Daten bzw. der Funktionsweise			
	Verfügbarkeit	Ein Ausfall des Systems, diverser Funktionen oder Anwendungen			
6. Verstoß gegen Gesetze, Vorschriften und/oder Verträge	Vertraulichkeit	Die unbefugte Preisgabe von Daten	...verstößt gegen Vorschriften oder Gesetze mit geringfügigen Konsequenzen. ...hat geringfügige Vertragsverletzungen mit Koventionalstrafen	...verstößt gegen Vorschriften oder Gesetze mit erheblichen Konsequenzen. ...hat Vertragsverletzungen mit Koventionalstrafen	...verstößt fundamental gegen Vorschriften oder Gesetze mit Konsequenzen. ...hat erhebliche Vertragsverletzungen mit Koventionalstrafe
	Integrität	Die Manipulation der Daten bzw. der Funktionsweise			
	Verfügbarkeit	Ein Ausfall des Systems, diverser Funktionen oder Anwendungen			

Schutzbedarfsfeststellung

Beeinträchtigungs-kategorien	Verlust von	Bedrohung	Schutzbedarfsfeststellung Kategorien		
			Abschätzung des Schadens		
			normal	hoch	sehr hoch
			kleiner als 5.000 € zur Folge.	zwischen 5.001 € und 50.000 € zur Folge.	n von mehr als 50.000 € zur Folge.

Tabelle 5: Individuelle Schutzbedarfskategorien

4.2 Schutzbedarf feststellung Geschäftsprozesse

In der folgenden Tabelle wird der Schutzbedarf für die Geschäftsprozesse anhand der vorstehenden Schadensszenarien und Grenzen der Schutzbedarfskategorien festgestellt.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
GP01	Konstruktion	Prozess der Erstellung, Revision und Ausarbeitung der digitalen Konzeption des Bauplans von Schiffen.	Hoch Technische Details zu bestimmten Komponenten oder Systemen, die wettbewerbsrelevant sein könnten.	Hoch Technische Details von kritischer Bedeutung für die Sicherheit und Funktionalität des Schiffs.	Hoch Daten und Informationen, die für den laufenden Bauprozess von entscheidender Bedeutung sind.
GP02	Einkauf	Prozess der Materialbeschaffung für die Konstruktion und Wartung von Schiffen	Hoch Die Preisgabe der Unternehmensdaten im Bereich des Einkaufs kann zu hohen Schäden führen z.B. durch Datenschutzklagen und Ansehensverlust.	Hoch Die unbemerkte/ungewollte Veränderung von Daten des Einkaufs z.B. Bestellungen von Material kann zu hohen Schäden führen durch ausstehende Zahlungen und Vertragsstrafen.	Hoch Ein Ausfall des Prozesses länger als 5 Tage kann nicht verkraftet werden, da sonst durch die Just in Time Produktion der Produktionsprozess abbricht.
GP03	Auftragsannahme / Verkauf	Prozess der Auftragsbearbeitung.	Hoch Die Preisgabe der Unternehmensdaten im Bereich des Verkaufs kann zu hohen Schäden führen z.B. durch Datenschutzklagen, Ansehensverlust und Vertragsstrafen. Die Preisgabe der Daten aus dem technischen Support können nur begrenzten Einfluss auf das Unternehmen nehmen.	Hoch Die unbemerkte/ungewollte Veränderung von Daten des Verkaufs z.B. Bestellungen von Schiffen kann zu hohen Schäden führen durch ausstehende Zahlungen und Vertragsstrafen, Stornierungen und Ansehensverlust. Die unbemerkte/ungewollte Veränderung der Daten des technischen Supports würden zu überschaubaren Nacharbeiten und Schäden führen.	Hoch Ein Ausfall des Verkaufsprozesses kann länger als 5 Tage verkraftet werden, da der Verkauf der Produktionsware mindestens 3 Wochen vor Fertigstellung abgewickelt wird. Ein Ausfall des Prozesses länger als 5 Tage kann nicht verkraftet werden, da sonst das Risiko steigt das der Produktionsprozess stagniert.

Schutzbedarfsfeststellung

GP04	Fertigung	Prozess der Bau und Wartung von Schiffen.	Sehr Hoch Die Preisgabe der Unternehmensgeheimnisse (z.B. Konstruktionspläne) können zu existenzbedrohenden Wettbewerbsnachteilen führen.	Sehr Hoch Die unbemerkte/ ungewollte Veränderung der Produktionsdaten z.B. Konstruktionspläne kann zu existenzbedrohendem Schaden für das Unternehmen führen.	Sehr Hoch Ein Ausfall der Produktion kann nicht über einen Zeitraum von 3 Tagen verkraftet werden und würde zu existenzbedrohenden Schaden innerhalb des Unternehmens führen.
GP05	Technischer Support	Der Prozess für die Bereitstellung von technischer Unterstützung und Lösungen Software, Hardware oder anderen IT-bezogenen Fragen.	Hoch Wenn im technischen Support sensible Informationen behandelt werden, die nicht für unbefugte Personen zugänglich sein dürfen, wie Mitarbeiterkontaktinformat vertrauliche Support-Tickets oder technische Details zur Produktion.	Hoch Wenn die Integrität der im Support behandelten Informationen von entscheidender Bedeutung ist, um sicherzustellen, dass Kunden korrekte und verlässliche technische Unterstützung erhalten.	Hoch Da der technische Support ununterbrochen verfügbar sein muss, um Mitarbeiter bei technischen Problemen zu unterstützen. Eine Nichtverfügbarkeit könnte zu erheblichen Beeinträchtigungen führen.

Tabelle 6: Schutzbedarfsfeststellung Geschäftsprozesse

4.3 Schutzbedarf feststellung Anwendungen

In der folgenden Tabelle wird der Schutzbedarf für die Anwendungen anhand der vorstehenden Schadensszenarien und Grenzen der Schutzbedarfskategorien festgestellt.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
A01	Excel	Excel ermöglicht es den Mitarbeitern, umfangreiche Datenmengen aus Produktion und Vertrieb zu verarbeiten, zu analysieren und zu präsentieren. Excel wird für die Erstellung von Produktionsplänen, Verkaufsprognosen und Budgets genutzt.	Hoch Excel wird intensiv für die Verarbeitung von vertraulichen Daten im Zusammenhang mit Schiffskonstruktionen verwendet.	Hoch Die Anwendung unterstützt den Schutz vor Datenverlust oder Manipulation durch regelmäßige Backups und Sicherheitsmechanismen.	Normal Durch andere Officeprodukte (Word) kann der Auffall dieser Anwendung länger toleriert werden. Verteilungseffekt.
A02	Outlook	Outlook ermöglicht es den Mitarbeitern, E-Mails zu senden und zu empfangen, wodurch die interne und externe Kommunikation erleichtert wird.	Hoch Outlook gewährleistet die Vertraulichkeit von E-Mails durch sichere Verschlüsselung und Zugriffskontrollen. Sensible Informationen werden geschützt, um unbefugten Zugriff zu verhindern.	Hoch Die Integrität von E-Mails und Daten wird durch fortgeschrittene Sicherheitsmechanismen sichergestellt, die sicherstellen, dass Informationen während der Übertragung und Speicherung unverändert bleiben.	Hoch Outlook bietet eine hohe Verfügbarkeit, sodass Benutzer jederzeit auf ihre E-Mails, Termine und Aufgaben zugreifen können. Die Anwendung wird durch robuste Serverinfrastrukturen unterstützt.
A03	Delftship	Delftship ist eine hochentwickelte Software für den Schiffsbau, die unseren Mitarbeitern eine umfassende Plattform für die digitale Konzeption von Schiffsbauplänen bietet.	Sehr Hoch Jeglicher unberechtigte Zugriff auf diese Daten könnte zu erheblichen Sicherheitsverletzungen führen, einschließlich potenzieller Gefährdung von	Sehr Hoch Jede Manipulation oder unbefugte Änderung dieser Daten könnten schwerwiegende Auswirkungen auf die Sicherheit und Leistungsfähigkeit der hergestellten Schiffe haben.	Sehr Hoch Aufgrund der zentralen Rolle, die Delftship bei der digitalen Konzeption des Bauplans von Schiffen spielt, sind Ausfälle nicht tolerierbar.

Schutzbedarf feststellung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
A04	TeamViewer	Die Software ermöglicht es Benutzern, auf sichere Weise von verschiedenen Standorten aus auf Computer und andere Geräte zuzugreifen.	Geschäftsgeheimnissen und geistigem Eigentum. Hoch Unternehmens- / Personendaten könnten einsehbar sein, wenn verwendet.	Normal Durch künftige Ablösung des Produkts ist kein besonderer Schutzbedarf notwendig.	Normal Durch künftige Ablösung des Produkts ist kein besonderer Schutzbedarf notwendig.
A05	Word	Microsoft Word ist eine weit verbreitete Textverarbeitungssoftware, die von den Abteilungen Produktion und Vertrieb in unserem Unternehmen genutzt wird.	Hoch Es besteht ein Risiko des unbefugten Zugriffs auf sensible Informationen. Dies könnte zu Datenlecks, Informationsverlust und potenziell rechtlichen Konsequenzen führen, wenn vertrauliche Geschäftsinformationen in die falschen Hände geraten.	Hoch Eine Beeinträchtigung der Integrität könnte zu fehlerhaften oder manipulierten Dokumenten führen, was wiederum zu falschen Entscheidungen und geschäftlichen Unregelmäßigkeiten führen könnte.	Normal Ein Ausfall des Prozesses länger als 5 Tage kann nicht verkraftet werden, da sonst das Risiko steigt das der Produktionsprozess stagniert.

Tabelle 7: Schutzbedarf feststellung Anwendungen

4.4 Schutzbedarf feststellung IT-Systeme

In der folgenden Tabelle wird der Schutzbedarf für die zum Einsatz kommenden IT-Systeme anhand der getroffenen Schutzbedarf feststellung für die Geschäftsprozesse und Anwendungen abgeleitet.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
AP1	WLAN Access Point Produktion		Normal Schutz interner Netzwerkinformationen im Bürobereich.	Hoch Sicherstellung ordnungsgemäßer Kommunikation im Bürobereich.	Hoch Sicherstellung einer kontinuierlichen Nutzung des Büro-WLANS.
AP2	WLAN Access Point Betrieb		Normal Schutz interner Netzwerkinformationen im Bürobereich.	Hoch Sicherstellung ordnungsgemäßer Kommunikation im Bürobereich.	Hoch Sicherstellung einer kontinuierlichen Nutzung des Büro-WLANS.
C1	Client Betrieb APC		Hoch Vererbung	Hoch Vererbung	V Normal Es gibt mehrere Clients, deswegen kann der Ausfall einer gewissen Anzahl verkraftet werden.
C1	Client Betrieb Laptop		Hoch Vererbung	Hoch Vererbung	V Normal Es gibt mehrere Clients, deswegen kann der Ausfall einer gewissen Anzahl verkraftet werden.
C2	Client Produktion		Sehr Hoch Vererbung	Sehr Hoch Vererbung	V Normal Es gibt mehrere Clients, deswegen kann der Ausfall einer gewissen Anzahl verkraftet werden.
C3	Client Produktionsleiter		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung
C4	Client Sekretär		Hoch Die Vertraulichkeit ist von entscheidender Bedeutung, da der Client wahrscheinlich sensible Informationen und Dokumente enthält. Der Zugriff sollte auf autorisierte Benutzer	Hoch Die Integrität des Clients ist entscheidend, um sicherzustellen, dass die auf dem Computer gespeicherten Dokumente und Informationen korrekt und unverändert bleiben.	Hoch Die Verfügbarkeit des Sekretär-Clients ist wichtig, um sicherzustellen, dass der Sekretär effizient arbeiten kann. Ausfälle könnten zu Arbeitsunterbrechungen und -verzögerungen führen.

Schutzbedarf feststellung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
C5	Client Geschäftsführung		beschränkt sein, um den Schutz vertraulicher Daten sicherzustellen. Sehr Hoch Der Client des Geschäftsführers enthält äußerst vertrauliche Informationen, wie Geschäftsstrategien, Finanzdaten und möglicherweise personenbezogene Daten. Der Zugriff sollte auf die höchsten Berechtigungsstufen beschränkt sein, um unbefugten Zugriff zu verhindern.	Manipulationen könnten zu falschen Informationen und Sicherheitsproblemen führen. Hoch Die Integrität der auf diesem Client gespeicherten Daten ist von entscheidender Bedeutung, um sicherzustellen, dass geschäftskritische Informationen nicht manipuliert oder verfälscht werden.	Hoch Die Verfügbarkeit dieses Clients ist wichtig, um sicherzustellen, dass der Geschäftsführer jederzeit auf relevante Informationen zugreifen kann. Ausfälle könnten die Effizienz und Reaktionsfähigkeit des Managements beeinträchtigen und sollten daher vermieden werden.
C6	Client CNC Fräse		Hoch Vererbung	Hoch Vererbung	Hoch Die Verfügbarkeit der Clients ist von entscheidender Bedeutung, um einen reibungslosen Produktionsprozess sicherzustellen. Ausfälle könnten zu Produktionsverzögerungen und -ausfällen führen.
C7	Client Gussmaschine		Hoch Vererbung	Hoch Vererbung	Sehr Hoch Die Verfügbarkeit der Clients ist von entscheidender Bedeutung, um einen reibungslosen Produktionsprozess sicherzustellen. Ausfälle könnten zu Produktionsverzögerungen und -ausfällen führen.
D1	Drucker Betrieb		Normal Drucker speichern normalerweise keine hochsensiblen Informationen.	Normal Die Integrität des Druckers bezieht sich darauf, dass er korrekte und unveränderte Druckaufträge ausführt. Manipulationen am Drucker könnten zu Fehldrucken oder unberechtigten Zugriffen auf Druckaufträge führen.	Hoch Die Verfügbarkeit des Druckers ist wichtig für den reibungslosen Geschäftsbetrieb. Ein Ausfall des Druckers könnte zu Verzögerungen in der Dokumentenverarbeitung führen.

Schutzbedarf feststellung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
D2	Drucker Produktion		Normal Produktionsdrucker in der Regel sind eher auf die Ausgabe von Produktionsdokumenten ausgerichtet, die normalerweise nicht als vertraulich gelten.	Normal Die Integrität ist wichtig, um sicherzustellen, dass Produktionsdokumente korrekt und unverändert ausgedruckt werden.	Hoch Die Verfügbarkeit des Produktionsdruckers ist entscheidend für einen effizienten Produktionsprozess. Ein Ausfall könnte zu Produktionsverzögerungen führen.
HP1	Switch Betrieb		Hoch Vererbung	Hoch Vererbung	K Sehr Hoch Sicherstellung einer kontinuierlichen Büronetzwerknutzung.
HP2	Switch Produktion		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Gewährleistung kontinuierlicher und zuverlässiger Produktionsabläufe.
N1	Firewall Betrieb	K	Sehr Hoch Da fast alle Anwendungen, sowie der DNS-Server, die Active Directory und der Webserver auf dem Server laufen, der die Verbindung zur Firewall hat.	Sehr Hoch Gewährleistung ordnungsgemäßer Firewall-Funktionen.	K Sehr Hoch Kontinuierlicher Schutz vor unbefugtem Zugriff.
N2	Firewall Produktion		Sehr Hoch Da fast alle Anwendungen, sowie der DNS-Server, die Active Directory und der Webserver auf dem Server laufen, der die Verbindung zur Firewall hat.	Sehr Hoch Gewährleistung ordnungsgemäßer Firewall-Funktionen.	Sehr Hoch Kontinuierlicher Schutz vor unbefugtem Zugriff.
R1	Router		Hoch Vererbung	Hoch Vererbung	Hoch Vererbung
S1	Server Betrieb		Hoch Vererbung	Hoch Vererbung	K Sehr Hoch Kummulationseffekt da fast alle Anwendungen, sowie der DNS-Server, die Active Directory und der Webserver auf dem Server laufen.
S2	Server Produktion		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung

Schutzbedarf feststellung

Tabelle 8: Schutzbedarf feststellung IT-Systeme

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
S100	SPS	Die SPS spielt eine entscheidende Rolle bei der Überwachung und Steuerung von Maschinen, Förderbändern und anderen produktionsrelevanten Abläufen.	Hoch Ein unbefugter Zugriff auf die SPS-Programmierung könnte zwar potenzielle Sicherheitsprobleme verursachen, ist jedoch in der Regel weniger kritisch als bei anderen Anwendungen.	Sehr Hoch Eine Beeinträchtigung der Integrität könnte zu schwerwiegenden Fehlfunktionen in der Produktionsanlage führen, was wiederum zu Qualitätsproblemen, Produktionsausfällen und Sicherheitsrisiken führen könnte.	Sehr Hoch Eine kontinuierliche Verfügbarkeit ist entscheidend, um einen reibungslosen Betrieb der Produktionsanlagen zu gewährleisten und Ausfallzeiten zu minimieren.
S101	Produktionsmaschine - CNC Fräse	Die CNC Fräse wird für die Herstellung von präzisen Bauteilen und Werkstücken aus verschiedenen Materialien wie Metall, Kunststoff oder Holz benutzt.	Hoch Der Zugriff auf die programmierbaren Codes und Designdaten muss auf autorisiertes Personal beschränkt sein, um die Integrität der Produktion und die geistigen Eigentumsrechte zu schützen.	Hoch Jegliche unbeabsichtigten oder böswilligen Änderungen an den Produktionscodes könnten zu fehlerhaften Produkten führen und müssen daher streng kontrolliert werden.	Sehr Hoch In kontinuierlichem Betrieb ist entscheidend, um Produktionsziele zu erreichen. Regelmäßige Wartung und sofortige Behebung von Störungen sind notwendig, um die Ausfallzeit zu minimieren.
S102	Produktionsmaschine - Gussmaschine		Hoch Der Zugang zu den spezifischen Gussparametern sollte beschränkt sein, um die Integrität der Gussproduktion zu wahren.	Hoch Jede Veränderung an den Gussparametern oder der Schmelztemperatur könnte die Qualität der produzierten Gussteile beeinträchtigen und muss daher streng überwacht werden.	Sehr Hoch Kontinuierlicher Betrieb und schnelle Reaktion auf Störungen sind entscheidend, um die Produktion effizient zu gestalten und

Schutzbedarf feststellung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
					Liefertermine einzuhalten.

Tabelle 15: Schutzbedarf feststellung ICS -Systeme

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
I1	Videoüberwachung		Hoch Daten können Informationen über Personen enthalten deshalb besonders Schützenswert	Hoch Änderung der Daten kann eine Straftat z.B. Diebstahl von Betriebsmitteln verschleiern	Normal Verteilungseffekt da es mehrere Kameras gibt kann der Ausfall einer gewissen Anzahl über einen kurzen Zeitraum verkraftet werden.
K1	Kaffeemaschine		Unkritisch Keine relevanten vertraulichen Informationen.	Unkritisch Geringe Auswirkung auf den Geschäftsbetrieb bei Ausfall oder Störungen.	Unkritisch Beeinflusst den Betrieb im Bürobereich, aber nicht kritisch für die Produktion.

Tabelle 16: Schutzbedarf feststellung IoT -Systeme

4.5 Schutzbedarf feststellung Kommunikationsverbindungen

In der folgenden Tabelle wird der Schutzbedarf für die Kommunikationsverbindungen zwischen den Komponenten im IT-Verbund festgelegt. Dies geschieht durch Ableitung des Schutzbedarfs der Geschäftsprozesse und Anwendungen sowie IT-Systeme die über diese Verbindungen kommunizieren.

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
AP1<>N	WLAN AP Betrieb <> Firewall Betrieb		M Unbearbeitet	M Unbearbeitet	M Unbearbeitet
AP2<>N	WLAN AP Produktion <> Firewall Produktion		M Unbearbeitet	M Unbearbeitet	M Unbearbeitet
C1/4/5	Client Betrieb <> WLAN AP Betrieb		Normal Vererbung	Hoch Vererbung	Hoch Vererbung
C1/4/5	Client Betrieb <> Firewall Betrieb		Hoch Vererbung	Hoch Vererbung	Hoch Verebung
C1<>C	Client Betrieb <> Client Produktion		Hoch Vererbung	Hoch Vererbung	Normal Vererbung
C1<>C	Client Betrieb <> Client Sekretär		Hoch Vererbung	Hoch Vererbung	Normal Vererbung
C1<>C	Client Betrieb <> Client Geschäftsführung		Hoch Vererbung	Hoch Vererbung	Hoch Vererbung
C1<>D	Client Betrieb <> Drucker Betrieb		Normal Vererbung	Normal Vererbung	Normal Vererbung
C1<>S1	Client Betrieb <> Server Betrieb		Hoch Vererbung	Hoch Vererbung	K Hoch Vererbung
C2/3/6	Client Produktion <> WLAN AP Produktion		Normal Vererbung	Hoch Vererbung	Hoch Vererbung
C2/3<>	Client Produktion/Produktions		Hoch Vererbung	Hoch Vererbung	Sehr Hoch Vererbung
C2/C3/	Client Produktion <> Firewall Produktion		Hoch Vererbung	Hoch Vererbung	Hoch Vererbung
C2<>C	Client Produktion <> Client Produktionsleiter		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung

Schutzbedarfsfeststellung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
C2>>C	Client Produktion<>Client CNC Fräse		Hoch Vererbung	Hoch Vererbung	Hoch Vererbung
C2>>C	Client Produktion<>Client Gussmaschine		Hoch Vererbung	Hoch Vererbung	Sehr Hoch Vererbung
C2>>D	Client Produktion<>Drucker Produktion		Normal Vererbung	Normal Vererbung	Hoch Vererbung
C2>>S2	Client Produktion<>Server Produktion		Sehr Hoch Da es sich um den Kernprozess der Werft handelt, ist die ordnungsgemäße und sichere Übertragung von Daten zwischen dem Produktionsclient und dem Produktionsserver entscheidend für die reibungslose Durchführung der Produktion von Schiffen.	Sehr Hoch Eine fehlerhafte Integrität könnte zu Produktionsfehlern oder Sicherheitsrisiken führen.	Sehr Hoch Jeder Ausfall oder jede Beeinträchtigung der Verfügbarkeit könnte zu erheblichen Produktionsverzögerungen führen.
C3>>D	Client Produktionsleiter<>Druck Produktion		Normal Vererbung	Normal Vererbung	Hoch Vererbung
C4>>C	Client Sekretär<>Client Geschäftsführung		Hoch Vererbung	Hoch Vererbung	Hoch Vererbung
C4>>D	Client Sekräter<>Drucker Betrieb		Normal Vererbung	Normal Vererbung	Hoch Vererbung
C5>>D	Client Geschäftsführung<>Druck Betrieb		Normal Vererbung	Normal Vererbung	Hoch Vererbung
HP1>>	Switch Betrieb<>WLAN AP Betrieb	M	Unbearbeitet	M	Unbearbeitet
HP1>>C	Switch Betrieb<>Client Betrieb	M	Hoch Vererbung	Hoch Vererbung	Sehr Hoch Vererbung
HP1>>	Switch Betrieb<>Drucker Betrieb	M	Unbearbeitet	M	Unbearbeitet
HP1>>N	Server Betrieb<>Firewall Betrieb	M	Unbearbeitet	M	Unbearbeitet
HP1>>S	Switch Betrieb<>Server Betrieb	M	Unbearbeitet	M	Unbearbeitet

Schutzbedarfsfeststellung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
HP2<->S	Switch Produktion<->WLAN AP Produktion		M Unbearbeitet	M Unbearbeitet	M Unbearbeitet
HP2<->C	Switch Produktion<->Client Produktion		Sehr Hoch Vererbung	Sehr Hoch Vererbung	Sehr Hoch Vererbung
HP2<->N	Switch Betrieb<->Firewall Betrieb		M Unbearbeitet	M Unbearbeitet	M Unbearbeitet
HP2<->S	Switch Produktion<->Drucker Produktion		M Unbearbeitet	M Unbearbeitet	M Unbearbeitet
HP2<->S	Switch Produktion<->Server Produktion		M Unbearbeitet	M Unbearbeitet	M Unbearbeitet
K40	Firewall Prod <-> Router		Hoch Der Schutz vor unbefugtem Zugriff auf diese Informationen ist entscheidend für die Sicherheit des Netzwerks.	Hoch Eine hohe Integrität schützt vor unautorisierten Änderungen, die die Netzwerksicherheit beeinträchtigen könnten.	Sehr Hoch Die Verfügbarkeit dieser Verbindung ist von entscheidender Bedeutung, da sie einen zentralen Punkt für die Netzwerkkommunikation darstellt.
K42	Router<->Videoüberwachung		Hoch Die Videoüberwachungskamera können sensible Bilder und Videos aufzeichnen.	Hoch Die Integrität der aufgezeichneten Videodaten ist wichtig, um sicherzustellen, dass die Informationen nicht manipuliert oder gefälscht werden	V Normal Jede Unterbrechung könnte zu Sicherheitslücken führen.
K43	Router<->Internet		Hoch Die Vertraulichkeit der Daten zwischen dem Router und dem Internet ist wichtig, um sensible Informationen vor unbefugtem Zugriff zu schützen.	Hoch Die Integrität der Daten ist entscheidend, um sicherzustellen, dass die Informationen während der Übertragung nicht	Sehr Hoch Die Verfügbarkeit ist von höchster Bedeutung, da eine kontinuierliche Verbindung zwischen dem Router und dem Internet sicherstellen muss, dass die Benutzer jederzeit auf die benötigten Ressourcen zugreifen können.

Schutzbedarfsfeststellung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
K44	Kaffeemaschine <> WLAN AP PROD		Unkritisch Spielt keine entscheidende Rolle.	Unkritisch manipuliert oder verändert werden.	Unkritisch Spielt keine entscheidende Rolle.
K45	Firewall Betrieb<->Router		Hoch Die Kommunikation zwischen Firewall und Router enthält sensible Informationen über die Netzwerkkonfiguration und Sicherheitsrichtlinien.	Hoch Die Integrität der Kommunikation zwischen Firewall Betrieb und Router ist von entscheidender Bedeutung.	Hoch Die ständige Verfügbarkeit der Kommunikation zwischen Firewall Betrieb und Router ist wesentlich für einen reibungslosen Netzwerkbetrieb.
K46	Firewall Betrieb<->Firewall Produktion		Hoch Zwischen den Firewalls werden sensible Sicherheitsinformationen ausgetauscht.	Hoch Die Integrität ist ebenfalls hoch, um sicherzustellen, dass keine unbefugten Änderungen an den Sicherheitsregeln oder -einstellungen vorgenommen werden.	Sehr Hoch Die Verfügbarkeit ist entscheidend, da eine unterbrochene Kommunikation zwischen den Firewalls schwerwiegende Auswirkungen auf die Sicherheit des Netzwerks haben kann.
S1<>N1	Server Betrieb<->Firewall Betrieb		Hoch Die Verbindung zwischen Server und Firewall enthält sensible Informationen.	Hoch Es ist wichtig sicherzustellen, dass die Informationen, die die Firewall passieren, nicht manipuliert werden.	Unbearbeitet Ausfälle könnten zu Sicherheitslücken führen.
S1<>S2	Server Betrieb<->Server Produktion		Hoch Die sensiblen Informationen werden zwischen den Servern übertragen.	Hoch Die Daten zwischen den Servern sollen korrekt und unverändert übertragen werden.	Hoch Die Verbindung zwischen den Servern ist geschäftskritisch und Ausfälle müssen vermieden werden.
S2<>N2	Server Produktion<->Firewall Produktion		Hoch	Hoch	Hoch

Schutzbedarf feststellung

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
			Die Verbindung zwischen Server und Firewall enthält sensible Informationen.	Es ist wichtig sicherzustellen, dass die Informationen, die die Firewall passieren, nicht manipuliert werden.	Ausfälle könnten zu Sicherheitslücken führen.

Tabelle 17: Schutzbedarf feststellung Kommunikationsverbindungen

5 Modellierung des Informationsverbunds

In diesem Abschnitt werden nun die Bausteine entsprechend den Objekten zugeordnet. Hierbei bietet es sich an Tabellen entsprechend der Schichten zu erstellen um die Modellierung übersichtlich zu gestalten.

5.1 Modellierung der IT-Systeme (Bausteine „alter“ Grundschutz)

In der Schicht der IT-Systeme werden die einzelnen, ggf. in Gruppen zusammengefassten, IT-Systeme des Informationsverbundes betrachtet.

Modellierung Grundschutzbausteine						
Bezeichnung	Titel des Bausteins	Reihenfolge	Relevanz	Zielobjekt	Begründung/Hinweise	Ansprechpartner
NET.3.1	Router und Switches		Ja	S1;S2		Leiter IT
SYS.1.2.3	Windows-Server		JA	S1;S2		Leiter IT
SYS.1.1	Allgemeiner Server		JA	S1;S2		Leiter IT

Tabelle 18: IT-Systeme nach IT-Grundschutz Modellierung der Anwendungen (Bausteine „alter“ Grundschutz)

In der Anwendungsschicht werden die Bausteine zu den jeweiligen Anwendungen der IT-Systeme zugeordnet

Modellierung Grundschutzbausteine						
Bezeichnung	Titel des Bausteins	Reihenfolge	Relevanz	Zielobjekt	Begründung/ Hinweise	Ansprechpartner
APP.1.1	Office-Produkte		JA	S1;S2		Externe Firma/Admin
OPS.1.2.5	Fernwartung		JA	S1;S2		Externe Firma

Tabelle 19: Anwendungen nach IT-Grundschutz Modellierung der Prozessbausteine (Vorgehen modernisierter Grundschutz)

Modellierung des Informationsverbunds

In der folgenden Tabelle sind die Prozessbausteine aufgeführt, welche für den gesamten KATRETTER-Verbund oder für weite Teile davon gelten.

Modellierung Grundschutzbausteine						
Bezeichnung	Titel des Bausteins	Reihenfolge	Relevanz	Zielobjekt	Begründung/ Hinweise	Ansprechpartner
DER.4	Notfallmanagement		JA	Gesamter Verbund		Geschäftsleitung
CON.9	Informationsaustausch		JA	Gesamter Verbund		Geschäftsleitung
CON.6	Löschen und Vernichten		JA	Gesamter Verbund		Geschäftsleitung
ORP.3	Sensibilisierung und Schulung zur Informationssicherheit		JA	Gesamter Verbund		Geschäftsleitung

Tabelle 20: Prozessbausteine Modellierung der Systembausteine

Nachfolgend werden die Systembausteine des modernisierten IT-Grundschutz zu den einzelnen IT-Systemen aufgelistet.

Modellierung Systembausteine						
Bezeichnung	Titel des Bausteins	Reihenfolge	Relevanz	Zielobjekt	Begründung/ Hinweise	Ansprechpartner
INF.7	Büroarbeitsplatz		JA	S1;S2		Geschäftsleitung
SYS.3.1	Laptops		JA	S1;S2		IT Abteilung

Tabelle 21: Systembausteine

6 IT-Grundschutz-Check

In diesem Abschnitt werden nun die Ergebnisse des IT-Grundschutzcheck also dem Soll-Ist-Vergleich der Anforderungen der modellierten Bausteine mit dem Umsetzungsstatus innerhalb des Verbunds. Hierbei gibt es eine Reihe von Tool die zur Unterstützung dienen. Ziehen Sie also Konsequenz aus den Ergebnissen des Checks und verweisen auf die Reportdatein des genutzten Tools. Oder auf die als Anlage genutzten Checklisten welche den Umsetzungsstatus ebenfalls dokumentieren, sollten Sie kein Tool genutzt haben.

Siehe Dokument:

[ITGS_A.4_Grundschutz-Check_Informationsverbund_2024-01-23.pdf](#)

7 Risikoanalyse

Ähnlich wie der Grundschutz-Check wird auch die Risikoanalyse durch Tools unterstützt somit können Sie auf diese Reports verweisen. Dennoch sollten das Ergebnis bzw. gewichtige Risiken hier aufgeführt werden.

Siehe Dokument:

[ITGS_A.5_Risikoanalyse_Informationsverbund_2024.pdf](#)

Notfallhandbuch

Hilfsmittel zum BSI-Standard 200-4

Dokumenteigenschaften

Kennzeichnung	Erläuterung
Titel	<i>Notfallhandbuch</i>
Klassifikation (Einstufung):	<i>Öffentlich Intern Vertraulich Streng-vertraulich</i>
Versionsnummer:	<i>1.0</i>
Zuständig:	<i>Jewgeni Sikorski (BCM-Beauftragter)</i>
Ablageort:	<i><Intranetlink>, Stabsraum, Battlebox, Büro des BCM-Beauftragten</i>
Zielgruppe / Verteiler:	<i>Alle BAO-Rollen</i>
Erstellt am:	<i>18.01.2024</i>
Erstellt von:	<i>Jewgeni Sikorski (BCM-Beauftragter)</i>
Letzte Überarbeitung:	<i>18.01.2024</i>
Nächste Überarbeitung:	<i>22.01.2024</i>
Freigabe am:	<i>24.01.2024</i>
Freigabe durch:	<i>Institutionsleitung</i>

Tabelle 1: Dokumenteigenschaften

Änderungshistorie

Version	Datum	Name	Beschreibung
0.9	18.01.2024	Jewgeni Sikorski (BCM-Beauftragter)	Ersterstellung
1.0	24.01.2024	Institutionsleitung	Freigegebene veröffentlichte Version

Tabelle 2: Änderungshistorie

Berlin 12459
Tel: +49 222 1111111111-0
E-Mail: s0561113@htw-berlin.de
Internet: <https://www.htw-berlin.de>

Inhalt

1	Einleitung.....	5
1.1	Zielsetzung	5
1.2	Geltungsbereich	5
1.3	Definitionen	5
1.4	Szenarien	6
2	Sofortmaßnahmen	7
2.1	Allgemeine Sofortmaßnahmen	7
2.2	Szenario-spezifische Sofortmaßnahmen.....	7
3	Alarmierung und Eskalation.....	10
3.1	Detektion und Meldung.....	10
3.2	Alarmierung der BAO.....	12
4	Wiederanlauf und Wiederherstellung.....	13
4.1	Wiederanlauf / Wiederherstellung nach Ausfall von Gebäuden und Gebäudeinfrastrukturen	13
4.2	Wiederanlauf / Wiederherstellung nach Ausfall von IT.....	14
4.3	Wiederanlauf / Wiederherstellung nach Ausfall von Personal.....	16
4.4	Wiederanlauf / Wiederherstellung nach Ausfall von Dienstleistern.....	17
5	Überführung in den Normalbetrieb	18
5.1	Erforderliche Maßnahmen zur Überführung	18
5.2	Deeskalation	18
5.3	Analyse und Bewertung der Notfallbewältigung	18
6	Überprüfung und Aktualisierung des Notfallhandbuchs	19

1 Einleitung

1.1 Zielsetzung

Dieses Dokument umfasst mit seinen Unterdokumenten alle Aspekte der Notfallbewältigung und kann auch für die Krisenbewältigung genutzt werden (ohne Rückgriff auf weiterführende Notfallpläne. Siehe auch Definition Notfall / Krise).

Das Notfallhandbuch soll die Zuständigen der SWDS in die Lage versetzen, einen geordneten Notbetrieb zu erreichen und die Rückkehr in den Normalbetrieb zu ermöglichen. Alle Regelungen, die den Notbetrieb in den Organisationseinheiten betreffen, sind in den weiterführenden Dokumenten zur Geschäftsförderung und zum Wiederanlauf / Wiederherstellung geregelt.

1.2 Geltungsbereich

Die Vorgaben des Notfallhandbuchs umfassen alle Standorte, Organisationseinheiten und Geschäftsprozesse gemäß Geltungsbereich des BCMS und sind für alle Rolleninhaber der BCM-BAO bindend.

1.3 Definitionen

Störung

Eine Störung ist eine Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen. Störungen werden in der Regel innerhalb des Normalbetriebs durch die Allgemeine Aufbauorganisation der Institution behoben. Hierzu wird auf vorhandene Prozesse zur Störungsbeseitigung oder des Incident-Managements zurückgegriffen.

Notfall

Notfälle sind Unterbrechungen des Geschäftsbetriebs, die mindestens einen zeitkritischen Geschäftsprozess betreffen, der nicht im Normalbetrieb innerhalb der maximal tolerierbaren Ausfallzeit wiederhergestellt werden kann. Im Gegensatz zu Störungen wird zur Bewältigung von Notfällen eine BAO benötigt. Im Gegensatz zur Krise liegen hier geeignete Pläne zur Bewältigung vor oder bestehende Pläne können adaptiert werden. Notfälle können auch eintreten, bevor das Schadensereignis zu einer Unterbrechung des Geschäftsbetriebs führt. Es genügt die Gefahr, dass durch das Schadensereignis der Geschäftsbetrieb unterbrochen wird.

Krise

Als Krise wird ein Schadensereignis bezeichnet, das sich in massiver Weise negativ auf die Institution auswirkt und dessen Auswirkungen auf die Institution nicht im Normalbetrieb bewältigt werden können. Im Gegensatz zu einem Notfall liegen zur Bewältigung einer Krise jedoch keine spezifischen Notfallpläne vor, vorhandene Notfallpläne können nicht oder nur bedingt adaptiert werden oder greifen schlicht nicht. Innerhalb der Institution wird die Krise durch eingeleitete Maßnahmen der BAO bewältigt.

1.4 Szenarien

Netzwerkausfall:

Am Montag beginnt wie regulär der Arbeitstag um 8 Uhr morgens. Jedoch liegt plötzlich ein Netzwerkausfall vor. Dadurch kann keiner mehr richtig arbeiten und es liegt ein Problem vor, dass nun zu lösen gilt.

Cyberangriff:

Über das Wochenende haben Cyberkriminelle sich in das System des Unternehmens gehackt und haben eine Ransomware-Schadprogramm installiert und alle Informationen verschlüsselt. Ein Mitarbeiter versucht sich am Montagmorgen anzumelden und bekommt ein Pop-Up Fenster, wo eine Geldsumme gefordert wird, sonst werden alle Daten gelöscht. Dasselbe Problem haben auch die anderen Mitarbeiter und selbst der Admin kommt nicht mehr in System rein. Nun liegt ein riesiges Problem vor, was zu lösen ist.

2 Sofortmaßnahmen

2.1 Allgemeine Sofortmaßnahmen

In einem Not- oder Krisenfall muss der Grundsatz beachtet werden, dass der Schutz von Leib und Leben vor dem Schutz von Sachwerten und Gütern steht. Sind Personen akut gefährdet, muss der Grundsatz beachtet werden: Umgebung sichern, Ereignis melden, Personen versorgen.

Hierunter fallen etwa:

- Sofortmaßnahmen zur Ersten Hilfe
- Sofortmaßnahmen zur Rettung und Bergung von Verletzten
- Sofortmaßnahmen bei Feuer
- Sofortmaßnahmen zur Räumung von Gebäuden und Betriebsstätten

Bei der Durchführung von Sofortmaßnahmen müssen folgende Grundsätze beachtet werden:

- Ruhe bewahren
- Eigenschutz geht vor
- Schutz von Leib und Leben hat oberste Priorität
- Durchsagen, insbesondere von Rettungskräften, muss Folge geleistet werden
- Vorgesetzte sind für die Sicherung ihrer Bereiche verantwortlich

Bei Gefahr für Leib und Leben müssen unmittelbar Rettungskräfte einbezogen werden. Rettungskräfte können wie folgt erreicht werden:

- <Feuerwehr / Rettungsdienst>
- <Polizei>
- <Werkschutz>
- <weitere>

2.2 Szenario-spezifische Sofortmaßnahmen

Zusätzlich zu den genannten Sofortmaßnahmen bestehen Szenario-spezifische Sofortmaßnahmen, die den Ausfall zeitkritischer Geschäftsprozesse bzw. Ressourcen verhindern oder die Auswirkungen eines Schadensereignisses eindämmen.

Sofortmaßnahmen bei Netzwerkausfall:

Nr.	Aktivität	Zuständig	Erledigt
1	Meldung des Schadensereignisses an Admin	Feststellende Person	
2	Fehlersuche und Schadensbegrenzung	Admin	
3	Beauftragung eines Wartungs- bzw. Reparaturdienstes	Admin	
4	Aktivierung von Backup-Kommunikationskanälen, falls vorhanden, um die Grundfunktionalität aufrechtzuerhalten.	Admin	
5	Aktuellen Arbeitsstand der zeitkritischen Geschäftsprozesse prüfen und Aufgaben priorisieren	Führungskräfte betroffener OEs	
6	Klare Anweisungen für die Wiederherstellung des Netzwerks, einschließlich der Verfahren zur Identifizierung und Behebung von Hardware- oder Konfigurationsproblemen.	Führungskräfte betroffener OEs	
7	Kommunikationsrichtlinien, um Mitarbeiter und Stakeholder über den Fortschritt der Fehlerbehebung zu informieren.	Führungskräfte betroffener OEs	
8	Überprüfung von Sicherheitsmaßnahmen, um sicherzustellen, dass der Ausfall nicht auf einen Sicherheitsvorfall zurückzuführen ist.	Admin	
9	Protokollierung aller Aktivitäten für spätere Bewertungen und Verbesserungen.	Admin	
10	Überwachung	Admin	

Tabelle 3: Sofortmaßnahmen bei Netzwerkausfall

Sofortmaßnahmen bei Ransomware

Nr.	Aktivität	Zuständig	Erledigt
1	Meldung des Schadensereignisses an Admin	Meldende Person	
2	Fehlersuche und Schadensbegrenzung	Admin	
3	Geschäftsführer kontaktieren und berichten	Admin	
4	Schnelle Isolierung der betroffenen Systeme, um die Ausbreitung des Angriffs zu verhindern.	Admin	
5	Einsatz von Backup- und Wiederherstellungsplänen zur Wiederherstellung von kritischen Daten und Systemen.	Admin	
6	Analyse der Angriffspunkte und Implementierung von Sicherheitspatches, um erneute Angriffe zu verhindern.	Admin/ externe Firma	
7	Einrichtung von Mechanismen zur Benachrichtigung von Behörden und Datenschutzbeauftragten gemäß den gesetzlichen Anforderungen.	Geschäftsführung	
8	Kommunikationsrichtlinien für die Informierung der Mitarbeiter, Kunden und Medien über den Vorfall.	Geschäftsführung	
9	Durchführung einer umfassenden forensischen Untersuchung, um die Ursache des Angriffs zu ermitteln und Maßnahmen zur Verhinderung zukünftiger Angriffe zu identifizieren	Admin / externe Firma	
10	Protokollierung aller Aktivitäten für spätere Bewertungen und Verbesserungen.	Admin / externe Firma	
11	Überwachung	Admin	

Tabelle 4: Sofortmaßnahmen Ransomware

3 Alarmierung und Eskalation

In der <Institution> gelten folgende Meldewege:

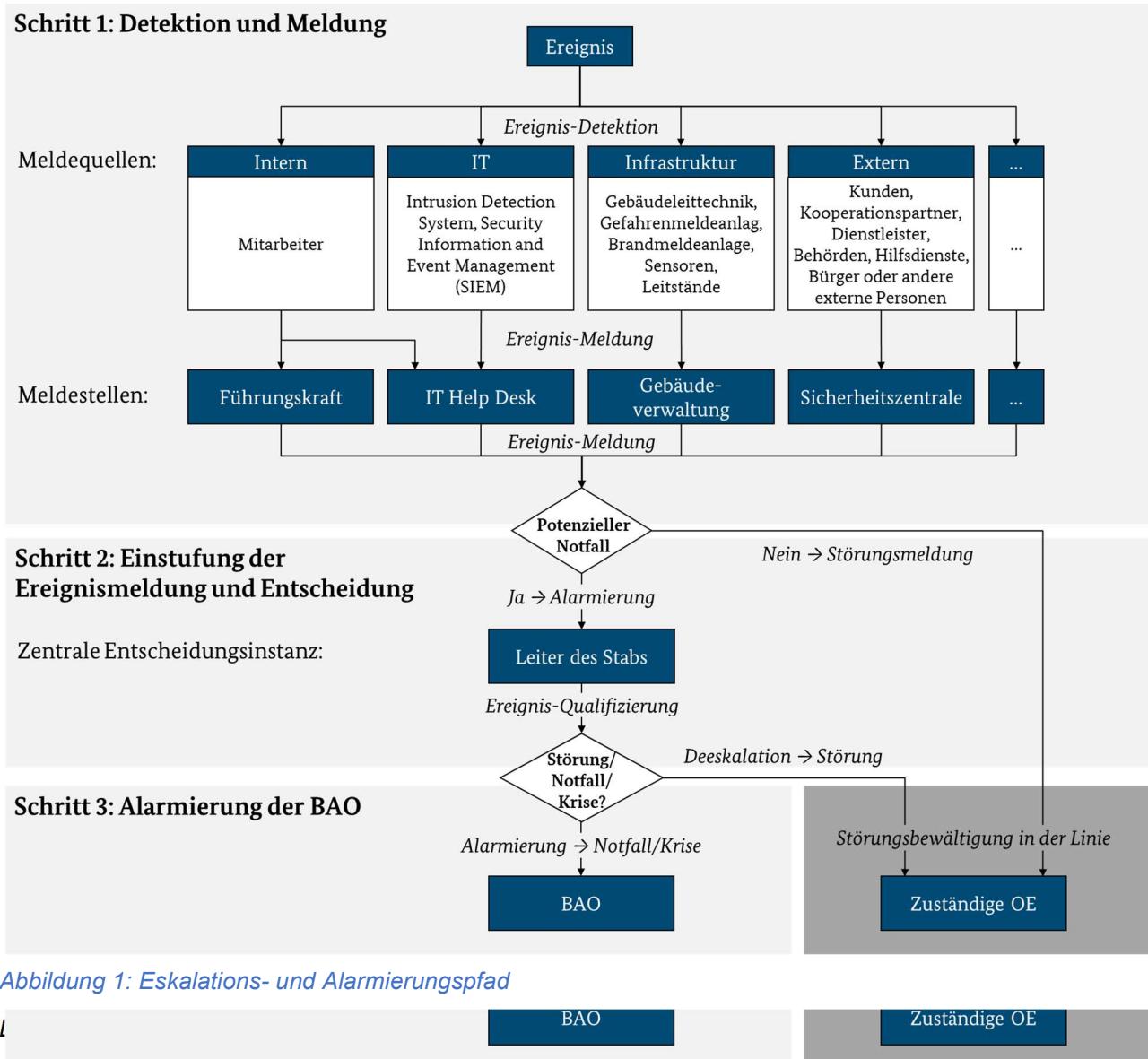


Abbildung 1: Eskalations- und Alarmierungspfad



Abbildung 1 kann als bearbeitbare Version als Hilfsmittel von der Seite des BSI bezogen werden.

Sollten die jeweiligen Ansprechpartner nicht erreichbar sein, müssen deren Stellvertreter gemäß Anhang alarmiert werden.

3.1 Detektion und Meldung

Die Ersteinschätzung eines Schadensereignisses erfolgt in den Meldestellen. Die Meldestellen können anhand der folgenden Leitfragen bewerten, ob das Ereignis Not- oder Krisenfallpotenzial hat. Wird das Schadensereignis als potenzieller Not- oder Krisenfall eingestuft, muss die zentrale Entscheidungsinstanz alarmiert werden. Falls die Meldestelle das Ereignis als Störung einstuft, die sich jedoch zu einem Not- oder Krisenfall entwickeln könnte, sollte die zentrale Entscheidungsstelle informiert und die Störung weiter beobachtet werden.

Meldestelle: Gebäudemanagement / Sicherheitszentrale / Sicherheitsdienstleister / Leitstand

Leitfragen für Schadensereignisse mit Not- oder Krisenfallpotenzial – Gebäude / Infrastruktur	Ja / Nein
<ul style="list-style-type: none"> • Ist / war die Räumung eines Gebäudes notwendig, z. B. aufgrund eines Brandes oder eines Sicherheitsvorfalls? • Kann oder darf mindestens ein Gebäudeteil (gesamte Etage, Brandabschnitt, Trakt etc.) zeitweise nicht genutzt werden, z. B. aufgrund eines Gebäudeschadens oder eines Defekts einzelner Infrastrukturkomponenten (Brandschutzeinrichtungen, Sanitäranlagen etc.)? • Ist die Versorgung mit Strom, Wasser oder Klimatisierung ausgefallen und eine ausreichend schnelle Wiederherstellung nicht absehbar? • Ist eine Produktionsmaschine oder -anlage ausgefallen und eine ausreichend schnelle Reparatur oder ein Ersatz nicht absehbar? • Ist die Sicherheit der Mitarbeiter am Standort aufgrund eines Ereignisses (z. B. Unwetterwarnung, politische Demonstration oder Schadensereignis im Umfeld) möglicherweise gefährdet? 	

*Sobald mindestens eine Frage mit JA beantwortet werden kann,
bitte umgehend den Leiter des Stabs alarmieren: Telefon 1234567890*

Tabelle 5: Leitfragen für Schadensereignisse mit Not- oder Krisenfall potenzial – Gebäude / Infrastruktur

Meldestelle: IT-Help Desk (1st / 2nd Level Support)

Leitfragen für Schadensereignisse mit Not- oder Krisenfallpotenzial – IT	Ja / Nein
<ul style="list-style-type: none"> • Ist das betroffene IT-System oder die betroffene Anwendung wesentlicher Bestandteil der Sicherheitsinfrastruktur (Viren-Management, Firewall etc.)? Für nähere Details siehe IT-Servicekatalog oder IT-Anwendungsliste. • Hat der Ausfall des betroffenen IT-Systems oder der betroffenen Anwendung Auswirkungen auf einen großen Nutzerkreis oder den wesentlichen Geschäftsbetrieb der Institution? • Besteht ein dringender Verdacht auf vorsätzliche Daten- oder Systemmanipulationen (Datenabfluss), unerlaubte Ausübung von Rechten oder eines gezielten Angriffs (physisch oder virtuell) auf IT-Komponenten? • Ist zu erwarten, dass die Auswirkungen des gemeldeten Ereignisses einen Zeitraum > X Stunden übersteigen werden? Gegebenenfalls die Information im 2nd Level Support erfragen. • Hat der Ausfall des betroffenen IT-Systems oder der betroffenen Anwendung Auswirkungen auf externe Interessengruppen, wie z. B. Kunden, Medien, Aufsichtsbehörden? Gegebenenfalls die Information beim Anwender erfragen. 	

*Sobald mindestens eine Frage mit JA beantwortet werden kann,
bitte umgehend den Leiter des Stabs alarmieren: Telefon 1234567890*

Tabelle 6: Leitfragen für Schadensereignisse mit Not- oder Krisenfallpotenzial – IT

Meldestelle: Führungskraft Personal

Leitfragen für Schadensereignisse mit Not- oder Krisenfallpotenzial – Personal	Ja / Nein
<ul style="list-style-type: none"> <i>Sind in Ihrem Zuständigkeitsbereich in Summe so viele Mitarbeiter nicht arbeitsfähig, dass Sie möglicherweise den Geschäftsbetrieb nicht mehr aufrechterhalten können?</i> <i>Ist durch die Abwesenheit von Mitarbeitern mit bestimmten Berechtigungen der normale Geschäftsbetrieb eventuell nicht mehr möglich?</i> 	

*Sobald mindestens eine Frage mit JA beantwortet werden kann,
bitte umgehend den Leiter des Stabs alarmieren: Telefon 1234567890*

Tabelle 7: Leitfragen für Schadensereignisse mit Not- oder Krisenfallpotenzial – Personal

Meldestelle: Provider Management bzw. Dienstleistersteuerung

Leitfragen für Schadensereignisse mit Not- oder Krisenfallpotenzial – Dienstleister	Ja / Nein
<ul style="list-style-type: none"> <i>Liegt beim Dienstleister oder dessen Subunternehmen ein nicht geplanter Ausfall bzw. Not- oder Krisenfall vor oder ist dieser absehbar?</i> <i>Hat der Dienstleister den Vertrag einseitig gekündigt und mit sofortiger Wirkung seine Leistung eingestellt?</i> 	

*Sobald mindestens eine Frage mit JA beantwortet werden kann,
bitte umgehend den Leiter des Stabs alarmieren: Telefon 1234567890*

Tabelle 8: Leitfragen für Schadensereignisse mit Not- oder Krisenfallpotenzial – Dienstleister

3.2 Alarmierung der BAO

Nach Meldung des Ereignisses an die zentrale Entscheidungsinstanz <Leiter des Stabs> muss dieser entscheiden, ob der Stab einberufen wird. Wenn ja, müssen umgehend die Mitglieder des Stabs in den Stabsraum oder die Telefonkonferenz einberufen werden.

Information der Stabsmitglieder über die Situation:

- Kurze Information zum Vorfall*
- Treffpunkt*
- [...]*

4 Wiederanlauf und Wiederherstellung

Der Wiederanlauf und die Wiederherstellung umfassten sämtliche Maßnahmen, Verfahren und weiterführenden Informationen, um ausgefallene Ressourcen schnellstmöglich wiederanlaufen oder wiederherstellen zu können. Der Wiederanlauf und die Wiederherstellung sind innerhalb von Wiederanlauf- und Wiederherstellungsplänen (WAPs / WHPs) dokumentiert und basieren auf den vorab definierten Business Continuity Strategien und Lösungen.

4.1 Wiederanlauf / Wiederherstellung nach Ausfall von Gebäuden und Gebäudeinfrastrukturen

Für den Wiederanlauf und die Wiederherstellung im Falle eines Gebäude- oder Gebäudeinfrastrukturausfalls gilt folgende BC-Strategie:

Zeitkritische Organisationseinheiten verlegen selbstständig gemäß GFP an die designierte Ausweichlokation. Nicht zeitkritische Organisationseinheiten oder Mitarbeiter nicht zeitkritischer Geschäftsprozesse werden für die Dauer der Notfall- und Krisenbewältigung nach Hause geschickt. Der Anlauf der Ausweichlokation sowie der Wiederanlauf des primären Standorts erfolgt über die folgenden WAPs / WHPs:

WAP / WHP	Beschreibung	Ansprechpartner / Kontakt	Verweis
WAP / WHP Gebäudeinfrastruktur	<p><i>Teams und Schlüsselpersonen festlegen,</i></p> <p><i>Geschäftsfunktionen die unerlässlich sind festlegen,</i></p> <p><i>Prioritätsreihenfolge festlegen,</i></p> <p><i>Standorte festlegen, welche man als alternative nutzen kann,</i></p> <p><i>Backups und Systeme am anderen Standort einspielen,</i></p> <p><i>Datensicherung kontrollieren,</i></p> <p><i>Plan für Mitarbeiter erstellen und Umzugspläne vorbereiten,</i></p> <p><i>Sicherstellen, dass am alternativen Standort das jeweilige Arbeitsmaterial vorliegt,</i></p> <p><i>Sicherheitsmaßnahmen prüfen und Zugangskontrolle,</i></p> <p><i>Dokumentation und Überwachung des weiteren Verlaufs</i></p>	<p><i>Gebäudemanagement</i></p> <p><i>Peter Schraubenzieher</i></p> <p><i>Festnetz: -500</i></p> <p><i>Mobil: 0124-476784</i></p>	<i>Link</i> <i>Physische Ablage</i>
...

Tabelle 9: Auflistung Wiederanlauf- und Wiederherstellungspläne nach Ausfall von Gebäuden und Gebäudeinfrastrukturen

4.2 Wiederanlauf / Wiederherstellung nach Ausfall von IT

Für den Wiederanlauf und die Wiederherstellung im Falle eines IT-Ausfalls gilt folgende BC-Strategie:

[...]

WAP / WHP	Beschreibung	Ansprechpartner / Kontakt	Verweis
WAP / WHP Standardarbeitsplatz	<p><i>Teams und zuständige Personen festlegen,</i></p> <p><i>Kommunikationskanäle festlegen intern/extern,</i></p> <p><i>unerlässliche Systeme und Anwendungen festlegen,</i></p> <p><i>Prioritätsreihenfolge festlegen,</i></p> <p><i>Backups prüfen und Wiederherstellung durch Backups einleiten,</i></p> <p><i>Wiederherstellung der wichtigsten Anwendungen zuerst, danach der Rest,</i></p> <p><i>Alle Prozesse sauber dokumentieren und Erkenntnisse ziehen,</i></p> <p><i>Systemüberwachung und Test festlegen</i></p>	<p><i>IT-Administrator/</i></p> <p><i>Festnetz: -500</i></p> <p><i>Mobil: 0124-456789</i></p>	<p><i>Link</i></p> <p><i>Physische Ablage</i></p>
...

Tabelle 10: Auslistung Wiederanlauf- und Wiederherstellungspläne nach Ausfall von IT

4.3 Wiederanlauf / Wiederherstellung nach Ausfall von Personal

Für den Wiederanlauf und die Wiederherstellung im Falle eines Ausfalls von Personal gilt folgende BC-Strategie:

[...]

WAP / WHP	Beschreibung	Ansprechpartner / Kontakt	Verweis
<i>Massenhafter Personalausfall</i>	<p><i>Identifizieren der unerlässlichen Anwendungen für den Betrieb,</i></p> <p><i>Teams/Personen festlegen, welche die wichtigsten Anwendungen vertreten,</i></p> <p><i>Verantwortlichkeiten übergaben, um Aufgaben zu erleichtern,</i></p> <p><i>flexible Ressourcenpläne schaffen und Teilzeitkräfte oder externe Dienstleister für den Zeitraum besorgen,</i></p> <p><i>Kommunikationswege festlegen,</i></p> <p><i>Mitarbeitern mit Maßnahmen helfen, um schneller gesund zu werden,</i></p> <p><i>Dokumentieren und Anpassen</i></p>	<p><i>Michael Holzhüter/</i></p> <p><i>Festnetz: -500</i></p> <p><i>Mobil: 0124-456785</i></p>	<p><i>Link</i></p> <p><i>Physische Ablage</i></p>
...

Tabelle 11: Auflistung Wiederanlauf- und Wiederherstellungspläne nach Ausfall von Personal

4.4 Wiederanlauf / Wiederherstellung nach Ausfall von Dienstleistern

Für den Wiederanlauf und die Wiederherstellung im Falle eines Ausfalls von Dienstleistern gilt folgende BC-Strategie:

[...]

WAP / WHP	Beschreibung	Ansprechpartner / Kontakt	Verweis
Notfallkonzept Lieferant A	<p>Dienstleistungen die unerlässlich sind festlegen,</p> <p>Prioritätsreihenfolge festlegen,</p> <p>Liste mit potenziellen alternativen Dienstleistern festlegen,</p> <p>Verträge und Vereinbarungen prüfen,</p> <p>Kommunikationswege erstellen, um den weiteren Verlauf besser zu kontrollieren,</p> <p>Dokumentation und Überwachung</p>	<p>Lieselotte Hans/ Festnetz: -500 Mobil: 0124-456782</p>	<p>Link Physische Ablage</p>
...

Tabelle 12: Auflistung Wiederanlauf- und Wiederherstellungspläne nach Ausfall von Personal

5 Überführung in den Normalbetrieb

Nach Überwindung des Schadenereignisses steuert der Stab die Überführung in den Normalbetrieb. Die Überführung unterteilt sich hierbei in die folgenden drei Phasen

- Erforderliche Maßnahmen zur Überführung
- Deeskalation
- Analyse und Bewertung der Notfall- und Krisenbewältigung

5.1 Erforderliche Maßnahmen zur Überführung

Vor der Deeskalation durch den Stab muss geprüft werden, ob die gravierenden Herausforderungen des Ereignisses gelöst wurden, übrige Nacharbeiten im Normalbetrieb erfolgen können und somit eine Überführung in den Normalbetrieb grundsätzliche möglich ist.

Der Stab muss prüfen, welche notwendigen Tätigkeiten veranlasst werden müssen, bis die Organisationseinheiten selbstständig ohne gesonderte Steuerung durch die BAO den Normalbetrieb wiederaufnehmen können. Mögliche Maßnahmen umfassen etwa die koordinierte Überführung von Mitarbeitern und Materialien an den Primärstandort oder das Abarbeiten von Arbeitsrückständen. Der Stab sollte intern (und ggf. auch extern) kommunizieren, wann die Überführung in den Normalbetrieb erwartet, sich der Stab auflösen und der Regelbetrieb wiederhergestellt sein wird.

5.2 Deeskalation

Nach Abschluss aller Tätigkeiten zur Überführung in den Normalbetrieb kann der Stab den Not- oder Krisenfall deeskalieren und den Normalbetrieb ausrufen. Dabei müssen folgende Hinweise beachtet werden:

- Nur der Stab kann den Not- oder Krisenfall deeskalieren.
- Sämtliche Sonderbefugnisse der Rollen innerhalb der besonderen Aufbauorganisation enden zum Zeitpunkt der Deeskalation.
- Zur Deeskalation müssen folgende Stellen informiert werden:
 - Mitarbeiter (per E-Mail und Durchsage)
 - Kunden (per E-Mail)
 - Medien (per Pressemitteilung)

5.3 Analyse und Bewertung der Notfallbewältigung

Nach der Rückkehr in den Normalbetrieb müssen die gewonnenen Erfahrungen aus der Notfall- und Krisenbewältigung anhand der Dokumentationen nachbereitet und der Institutionsleitung berichtet werden. Informationen wie beispielsweise aufgetretene Probleme in der Notfall- und Krisenbewältigung können als Grundlage für eine Überarbeitung und Aktualisierung des BCM-Prozesses genutzt werden. Der <BCM-Beauftragte> muss die zeitgerechte Umsetzung der Verbesserungsmaßnahmen überwachen und der <Institutionsleitung> regelmäßig Bericht erstatten. [...]

6 Überprüfung und Aktualisierung des Notfallhandbuchs

Mindestens Jährlich muss der BCMB das Notfallhandbuch hinsichtlich Aktualität und Angemessenheit überprüfen. Bei wesentlichen Änderungen an den Rahmenbedingungen des BCM oder Erkenntnissen aus eingetretenen Not- und Krisenfällen sowie Tests und Übungen muss das Notfallhandbuch anlassbezogen aktualisiert werden.

Das Notfallhandbuch wird durch die Institutionsleitung freigegeben und ersetzt vorherige Versionen. Die aktualisierte Version muss der Zielgruppe / dem Verteiler des Notfallhandbuchs bekanntgegeben werden. [...]

Datenschutz-Checkliste

	Checkliste	Haben Sie das bereits umgesetzt? JA / NEIN / TEILWEISE	Maßnahmen zur Umsetzung	Priorität HOCH/ MITTEL/ NIEDRIG
1	Wird die Unabhängigkeit des Datenschutzbeauftragten sichergestellt, um Interessenskonflikte zu vermeiden?	JA/ NEIN / TEILWEISE	DSB geschützt durch Art. 38 Abs. 3 DSGVO darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Außerdem durch § 6 Abs. 4 BDSG , Kündigung nicht einfach möglich.	Hoch
2	Finden regelmäßige Schulungen zum Datenschutz statt?	JA/ NEIN / TEILWEISE	Es gibt eine Schulung welche sich Allgemein mit solchen Dingen beschäftigt aber nicht speziell mit Datenschutz, daher muss hier ein neues Schulungskonzept etabliert werden.	Mittel
3	Sind auf allen Systemen Firewalls und Schutz von Schadsoftware installiert, aktiviert?	JA/ NEIN / TEILWEISE	Linux: Bitdefender, Microsoft: MS-Defender, Sophos Firewall	Hoch
4	Gibt es ein Datenschutzkonzept?	JA/ NEIN / TEILWEISE	Datenschutzkonzept nach DSGVO erstellen	Hoch
5	Sind Firewalls und Schutzsoftware immer auf dem aktuellen Stand?	JA/ NEIN / TEILWEISE	Aktualisierung findet immer statt sobald ein Update oder Patch veröffentlicht wird.	Hoch
6	Gibt es eine Passwortrichtlinie?	JA/ NEIN / TEILWEISE	Groß- und Kleinbuchstaben, Mindestens eine Zahl, Mindestens ein Sonderzeichen, Mindestens 10 Zeichen Bsp.: rWz{q)?V?	Hoch
7	Gibt es ein Konzept für Zugriffsberechtigung (Gebäude)?	JA/ NEIN / TEILWEISE	FiBu darf nur FiBu Raum, Werkstattmitarbeiter nicht in FiBu Raum etc.	Hoch
8	Gibt es eine Benutzer Authentifikation?	JA/ NEIN / TEILWEISE	Umsetzung durch AD Richtlinie	Hoch
9	Gibt es Zugriffsrechte für bestimmte Tätigkeitsprofile?	JA/ NEIN / TEILWEISE	Umsetzung durch Grp.-Richtlinie	Hoch
10	Werden Verletzungen und Verstöße beim Datenschutz im Unternehmen protokolliert?	JA/ NEIN / TEILWEISE	Elektronisches Protokoll zum vermerken von Vorfällen mit Zeit Stempel, Personal ID, Vorfall, Auswirkung etc.	Mittel
11	Werden Datenträger/Datenblätter sicher aufbewahrt? (Personal)	JA/ NEIN / TEILWEISE	Jeder Mitarbeiter soll sensibilisiert werden seine Datenträge weg zu schließen und sensible Datenblätter nach Gebrauch in Aktenschränke zu verstauen.	Hoch
12	Werden Datenträger/Datenblätter sicher entsorgt?	JA/ NEIN / TEILWEISE	Datenblätter werden geschreddert und Datenträger Formatiert und entsorgt. Es muss ein Konzept entworfen werden für vollständige Zerstörung der Datenträger.	Hoch

13	Wurde ein entsprechender Kopierschutz/Bearbeitungsschutz eingerichtet?	JA/ NEIN / TEILWEISE	Besitzer ist Ersteller bei Bearbeitung wird ähnlich wie bei Git nochmal vom Ersteller drüber geschaut und dann genehmigt.	
14	Findet die regelmäßige Kontrolle der Fristen zur Löschung personenbezogener Daten statt?	JA/ NEIN / TEILWEISE	Nach DSGVO, einen Monat um den Antrag zu prüfen. Dann unverzüglich ohne schuldhaftes Zögern. Bei gesetzlicher oder steuerrechtlicher Aufbewahrungspflicht, nach Ablauf der Frist. Bewerkstelligt durch ein automatisiertes Löschkonzept	Hoch
15	Werden die Daten rechtzeitig gelöscht?	JA/ NEIN / TEILWEISE	Automatisiertes Löschkonzept	Hoch
16	Ist die Übermittlung von Daten durch Verschlüsselung und andere Sicherheitsmaßnahmen vor dem unbefugten Abgreifen geschützt?	JA/ NEIN / TEILWEISE	Mails sind durch TLS von Microsoft verschlüsselt. S/MIME wäre noch in Betracht zu ziehen, muss aber von end zu end eingerichtet sein. Interne Wichtige Daten sind verschlüsselt und durch Passwörter gesichert.	Hoch
17	Gibt es eine umfassende schriftliche Dokumentation über die technisch organisatorischen Maßnahmen (TOM)?	JA/ NEIN / TEILWEISE	https://dsgvo-vorlagen.de/tom-nach-dsgvo-richtig-dokumentieren	Hoch
18	Gibt es entsprechende Leitlinien zur Informationssicherheit und der Nutzung der IT-Systeme?	JA/ NEIN / TEILWEISE		
19	Existiert ein Notfallplan (für den Fall von Datenlecks, Infiltration von Schadsoftware, Missbrauch usf.)?	JA/ NEIN / TEILWEISE	Siehe Notfallplan	Hoch
20	Existiert eine rechtssichere Datenschutzerklärung für Ihr Unternehmen?	JA/ NEIN / TEILWEISE	Siehe Datenschutzerklärung	Hoch