Inhalt

ISMS – Tabelle:

A.5 – Sicherheitspolitik

A.5.1Politik zur Informationssicherheit

A.5.1 Politik zur Informationssicherheit *Ziel:* Richtungsvorgabe und Unterstützung des Managements bei der Informationssicherheit in Übereinstimmung mit den Geschäftsanforderungen und geltenden Gesetzen und behördliche Anforderungen.		
A.5.1.1	Dokument zur InformationssicherheitPolitik	*Maßnahme* Das Management muss eine InformationssicherheitsPolitik genehmigen, veröffentlichen und alle Mitarbeiter*innen und relevanten Externen davon in Kenntnis setzen.
A.5.1.2	Überprüfung der Informationssicherheits-Politik	*Maßnahme* Die Informationssicherheits-Politik muss in regelmäßigen Abständen oder, wenn wesentliche Änderungen erfolgen, überprüft werden, um ihre Eignung, Angemessenheit und Wirksamkeit auf Dauer sicherzustellen.

A.6 – Organisation der Informationssicherheit

A.6.1 Interne Organisation

A.6.1 Interne Organisation *Ziel:* Management der Informationssicherheit innerhalb der Organisation.		
A.6.1.1	Engagement des Managements für Informationssicherheit	*Maßnahme* Das Management muss die Informationssicherheit innerhalb der Organisation aktiv unterstützen, indem es eine klare Ausrichtung vorgibt, sein Engagement demonstriert, Rollen explizit formuliert und die Verantwortlichkeiten für Informationssicherheit anerkennt.
A.6.1.2	Koordination der Informationssicherheit	*Maßnahme* Aktivitäten im Rahmen der Informationssicherheit müssen durch Repräsentanten verschiedener Organisationsbereiche mit relevanten Aufgabenbereichen und Funktionen koordiniert werden.
A.6.1.3	Zuweisung der Verantwortlichkeiten für Informationssicherheit	*Maßnahme* Alle Verantwortlichkeiten für Informationssicherheit müssen eindeutig definiert sein.
A.6.1.4	Genehmigungsprozess für informationsverarbeitende Einrichtungen	*Maßnahme* Für neue informationsverarbeitende Einrichtungen muss ein Genehmigungsprozess durch das Management festgelegt und umgesetzt werden.
A.6.1.5	Vertraulichkeits- oder Geheimhaltunsvereinbarungen	*Maßnahme* Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, die den Schutzbedarf der Organisation für Informationen widerspiegeln, müssen identifiziert und regelmäßig überprüft werden.
A.6.1.6	Kontakt zu Behörden	*Maßnahme* Geeignete Kontakte zu relevanten Behörden müssen gepflegt werden.
A.6.1.7	Kontakt zu speziellen Interessensgruppen	*Maßnahme* Geeignete Kontakte zu speziellen Interessensgruppen oder anderen Experten-

		Sicherheitsforen und professionellen Verbänden müssen gepflegt werden.
A.6.1.8	Unabhängige Überprüfung der Informationssicherheit	*Maßnahme* Der Ansatz einer Organisation zum Management von Informationssicherheit und deren Umsetzung (d. h. Maßnahmenziele, Maßnahmen, Politik, Prozesse und Verfahren für Informationssicherheit) muss in regelmäßigen Zeitabständen oder nach wesentlichen Änderungen an der Sicherheitsimplementierung von unabhängiger Seite überprüft werden.

A.6.2 - Externe

A.6.2 Externe *Ziel:* Aufrechterhaltung der Sicherheit organisationseigener Informationen und informationsverarbeitender Einrichtungen, die von Externen benutzt werden, für sie zugänglich sind, an Externe kommuniziert werden oder durch sie verwaltet werden.		
A.6.2.1	Identifizierung von Risiken in Zusammenhang mit Externen	*Maßnahme* Die Risiken für organisationseigene Informationen und informationsverarbeitende Einrichtungen, die durch Geschäftsprozesse mit Externen verknüpft sind, müssen identifiziert werden und angemessene Maßnahmen müssen umgesetzt werden, bevor der Zugriff gewährt wird.
A.6.2.2	Adressieren von Sicherheit im Umgang mit Kunden	*Maßnahme* Alle identifizierten Sicherheitsanforderungen müssen berücksichtigt sein, bevor Kunden Zugang zu Informationen oder Vermögenswerten der Organisation gewährt wird.
A.6.2.3	Adressieren von Sicherheit in Vereinbarungen mit Dritten	*Maßnahme* Vereinbarungen mit Dritten, welche den Zugriff, die Verarbeitung, Kommunikation oder Administration von Informationen oder informationsverarbeitenden Einrichtungen der Organisation oder die Bereitstellung von Produkten oder Dienstleistungen für informationsverarbeitende Einrichtungen betreffen, müssen alle relevanten Sicherheitsanforderungen abdecken.

A.7 – Management von Vermögenswerten

A.7.1 – Verantwortlichkeit für Vermögenswerte

A.7.1 Verantwortlichkeit für Vermögenswerte *Ziel:* Erreichung und Erhaltung des angemessenen Schutzes von organisationseigenen Vermögenswerten.		
A.7.1.1	Inventar der Vermögenswerte	*Maßnahme* Alle Vermögenswerte müssen eindeutig identifiziert werden und ein Inventar aller wichtigen Vermögenswerte muss erstellt und instand gehalten werden.
A.7.1.2	Eigentum von Vermögenswerten	*Maßnahme* Alle Informationen und Vermögenswerte in Verbindung mit informationsverarbeitenden Einrichtungen müssen einem bestimmten Teil der Organisation als Eigentümer*innen[1] dieser Vermögenswerte zugeordnet sein.
A.7.1.3	Zulässige Nutzung von Vermögenswerten	*Maßnahme* Regeln für die zulässige Nutzung von Informationen und Vermögenswerten in Verbindung mit informationsverarbeitenden Einrichtungen müssen identifiziert, dokumentiert und umgesetzt werden.

A.7.2 – Klassifizierung von Informationen

A.7.2 Klassifizierung von Informationen *Ziel:* Sicherstellung des angemessenen Schutzes von Informationen.		
A.7.2.1	Richtlinien für die Klassifizierung	*Maßnahme* Informationen müssen bezüglich ihres Werts, gesetzlicher Anforderungen, Sensibilität und Kritikalität für die Organisation klassifiziert werden.
A.7.2.2	Kennzeichnung von und Umgang mit Informationen	*Maßnahme* Geeignete Verfahren für die Kennzeichnung von und den Umgang mit Informationen müssen in Übereinstimmung mit dem von der Organisation angewendeten Klassifizierungsschema entwickelt und umgesetzt werden.

A.8 – Personelle Sicherheit

A.8.1 – Vor Beginn der Beschäftigung

A.8.1 Vor Beginn der Beschäftigung[2] *Ziel:* Sicherstellung, dass Mitarbeiter*innen, Auftragnehmer*innen und Dritte ihre Verantwortlichkeiten verstehen und für die vorgesehenen Rollen geeignet sind und die Risiken durch Diebstahl, Betrug oder Missbrauch von Einrichtungen verringern.		
A.8.1.1	Rollen und Verantwortlichkeiten	*Maßnahme* Sicherheitsrollen und -verantwortlichkeiten von Mitarbeiter*innen*innen, Auftragnehmer*innen und Dritten müssen im Einklang mit den Informationssicherheits-Grundsätzen der Organisation definiert und dokumentiert werden.
A.8.1.2	Überprüfung	*Maßnahme* Überprüfungen des Hintergrunds aller Bewerber*innen, Auftragnehmer*innen und Dritten müssen in Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen ausgeführt werden, und sie müssen den Geschäftsanforderungen, der Klassifizierung der Informationen, die diese verwenden werden, und den erkannten Risiken angemessen sein.
A.8.1.3	Beschäftigungsbedingungen	*Maßnahme* Als Teil ihrer vertraglichen Auflagen müssen Mitarbeiter*innen, Auftragnehmer*innen und Dritte den Bedingungen des Beschäftigungsvertrags zustimmen und diesen unterzeichnen; diese Bedingungen müssen ihre und die Verantwortlichkeiten der Organisation für die Informationssicherheit festlegen.

A.8.2 – Während der Beschäftigung

A.8.2 Während der Beschäftigung *Ziel:* Sicherstellung, dass sich Mitarbeiter*innen, Auftragnehmer*innen und Dritte der Informationssicherheits-Bedrohungen und -Bedenken sowie ihrer Verantwortlichkeiten und Pflichten bewusst sind und dass sie in der Lage sind, die organisationseigene Sicherheitspolitik im Rahmen ihrer normalen Arbeit zu befolgen und das Risiko von menschlichen Fehlern verringern.		
		Maßnahme

A.8.2.1	Verantwortlichkeit des Managements	Das Management muss verlangen, dass sich Mitarbeiter*innen, Auftragnehmer*innen und Dritte der Sicherheit in Übereinstimmung mit den festgelegten Anweisungen und Verfahren der Organisation widmen.
A.8.2.2	Bewusstsein, Ausbildung und Schulung für Informationssicherheit	*Maßnahme* Alle Mitarbeiter*innen der Organisation und, falls relevant, Auftragnehmer*innen und Dritte, müssen entsprechende bewusstseinsbildende Schulung und regelmäßige aktualisierte Informationen über Politik und Verfahren der Organisation erhalten, sofern diese für ihre Arbeit von Bedeutung sind.
A.8.2.3	Disziplinarverfahren	*Maßnahme* Für Mitarbeiter*innen, die einen Sicherheitsverstoß begangen haben, muss ein formales Disziplinarverfahren eingeleitet werden.

A.8.3 – Auflösung oder Änderung der Beschäftigung

A.8.3 Auflösung oder Änderung der Beschäftigung *Ziel:* Sicherstellung, dass Mitarbeiter*innen, Auftragnehmer*innen und Dritte die Organisation ordnungsgemäß verlassen oder die Beschäftigung ordnungsgemäß wechseln.		
A.8.3.1	Verantwortlichkeiten bei der Beendigung	*Maßnahme* Die Verantwortlichkeiten für das Beenden oder Ändern einer Beschäftigung müssen klar definiert und zugewiesen werden.
A.8.3.2	Rückgabe von Vermögenswerten	*Maßnahme* Alle Mitarbeiter*innen, Auftragnehmer*innen und Dritte müssen alle organisationseigenen Vermögenswerte in ihrem Besitz bei der Beendigung ihrer Beschäftigung, ihres Vertrags oder ihrer Vereinbarung zurückgeben.
A.8.3.3	Aufheben von Zugangsbzw. Zugriffsrechten	*Maßnahme* Zugangsbzw. Zugriffsrechte aller Mitarbeiter*innen, Auftragnehmer*innen und Dritten auf Informationen und informationsverarbeitende Einrichtungen müssen aufgehoben werden, wenn ihre Anstellung,

		Vertrag oder Vereinbarung endet oder sie müssen bei Veränderungen angepasst werden.

A.9 - Physische und umgebungsbezogene Sicherheit

A.9.1 - Sicherheitsbereiche

A.9.1 Sicherheitsbereiche *Ziel:* Verhinderung von unerlaubtem Zutritt zu, Beschädigung und Störung von Organisationsinfrastruktur und der Organisation gehörenden Informationen.		
A.9.1.1	Physische Sicherheitsaußengrenzen	*Maßnahme* Sicherheitsaußengrenzen (Hindernisse wie Wände, über Zutrittskarten kontrollierte Zugänge oder mit Pförtnern besetzte Empfangsbereiche) müssen festgelegt werden, um die Bereiche zu schützen, welche Informationsspeicher und informationsverarbeitende Einrichtungen beherbergen.
A.9.1.2	Physische Zutrittskontrollen	*Maßnahme* Sicherheitsbereiche müssen durch angemessene Zutrittskontrollen geschützt werden, um sicherzustellen, dass nur autorisiertem Personal Zutritt gewährt wird.
A.9.1.3	Sicherung von Büros, Räumen und Einrichtungen	*Maßnahme* Physischer Schutz für Büros, Räume und Einrichtungen muss geplant und umgesetzt werden.
A.9.1.4	Schutz vor äußeren und umweltbedingten Bedrohungen	*Maßnahme* Physischer Schutz gegen Feuer, Wasser, Erdbeben, Explosionen, Unruhen und andere Formen natürlicher oder von Menschen verursachter Katastrophen muss vorgesehen und umgesetzt werden.
A.9.1.5	Arbeit in Sicherheitsbereichen	*Maßnahme* Physischer Schutz und Richtlinien für die Arbeit in Sicherheitsbereichen müssen entwickelt und umgesetzt werden.
		Maßnahme Zutrittspunkte wie Lieferund Ladebereiche sowie andere Punkte, an denen unbefugte Personen die

A.9.1.6	Öffentlicher Zutritt, Lieferund Ladebereiche	Geschäftsräume betreten können, müssen kontrolliert und, sofern möglich, von informationsverarbeitenden Einrichtungen getrennt werden, um unerlaubten Zugriff darauf zu verhindern.

A.9.2 – Sicherheit von Geräten

A.9.2 Sicherheit von Geräten *Ziel:* Verhinderung des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Vermögenswerten und Unterbrechung der Aktivitäten einer Organisation.		
A.9.2.1	Platzierung und Schutz von Geräten	*Maßnahme* Geräte müssen so platziert oder geschützt werden, dass das Risiko durch Bedrohungen aus Umwelt, Katastrophen sowie Gelegenheiten zu unerlaubtem Zugriff reduziert wird.
A.9.2.2	Unterstützende Versorgungseinrichtungen	*Maßnahme* Geräte müssen vor Stromausfällen und Ausfällen anderer Versorgungseinrichtungen geschützt werden.
A.9.2.3	Sicherheit der Verkabelung	*Maßnahme* Netz- und Telekommunikations-Verkabelungen, welche Daten übertragen oder die Informationssysteme versorgen, müssen vor Abhören oder Beschädigung geschützt werden.
A.9.2.4	Instandhaltung von Geräten	*Maßnahme* Geräte müssen korrekt gewartet werden, um ihre kontinuierliche Verfügbarkeit und Integrität sicherzustellen.
A.9.2.5	Sicherheit von außerhalb des Standorts befindlichen Geräten	*Maßnahme* Geräte, die sich außerhalb des Standorts befinden, müssen unter Beachtung der unterschiedlichen Risiken, die durch den Einsatz außerhalb eines Standorts entstehen, geschützt werden.
A.9.2.6	Sichere Entsorgung oder Weiterverwendung von Geräten	*Maßnahme* Bei allen Teilen von Geräten, die Speichermedien enthalten, muss vor der Entsorgung überprüft werden, ob alle sensiblen Daten und lizenzierte

		Software entfernt oder sicher überschrieben wurden.
A.9.2.7	Entfernung von Eigentum	*Maßnahme* Geräte, Informationen oder Software dürfen nicht unberechtigt vom Standort entfernt werden.

A.10 - Management der Kommunikation und des Betriebes

A.10.1 – Betriebsverfahren und Verantwortlichkeiten

A.10.1 Betriebsverfahren und Verantwortlichkeiten *Ziel:* Sicherstellung des korrekten und sicheren Betriebs von informationsverarbeitenden Einrichtungen.		
A.10.1.1	Dokumentierte Betriebsverfahren	*Maßnahme* Betriebsverfahren müssen dokumentiert, gewartet und allen Benutzern, die sie benötigen, verfügbar gemacht werden.
A.10.1.2	Änderungsmanagement	*Maßnahme* Änderungen an informationsverarbeitenden Einrichtungen und Systemen müssen kontrolliert erfolgen.
A.10.1.3	Aufgabentrennung	*Maßnahme* Aufgaben und Verantwortungsbereiche müssen getrennt werden, um die Gelegenheit für unbefugte oder vorsätzliche Veränderung oder Missbrauch von organisationseigenen Vermögenswerten zu reduzieren.
A.10.1.4	Funktionstrennung von Entwicklungs-, Testund Produktionseinrichtungen	*Maßnahme* Entwicklungs-, Test- und Produktionseinrichtungen müssen getrennt werden, um das Risiko unbefugten Zugriffs oder Änderungen des Produktionssystems zu verhindern.

A.10.2 – Management der Erbringung von Dienstleistungen durch Dritte

A.10.2 Management der Erbringung von Dienstleistungen durch Dritte *Ziel:* Umsetzung und Aufrechterhaltung eines angemessenen Grades an Informationssicherheit sowie Erbringung von Dienstleistungen in Übereinstimmung mit den Liefervereinbarungen mit Dritten.		
A.10.2.1		*Maßnahme* Es muss sichergestellt sein, dass die Sicherheitsmaßnahmen, Festlegung der Leistungen und Lieferumfang, die in der Liefervereinbarung mit Dritten enthalten sind, von

	Erbringung von Dienstleistungen	den Dritten umgesetzt, durchgeführt und eingehalten werden.
A.10.2.2	Überwachung und Überprüfung der Dienstleistungen von Dritten	*Maßnahme* Die von Dritten gelieferten Dienstleistungen, Berichte und Aufzeichnungen müssen regelmäßig überwacht und überprüft werden und Audits müssen regelmäßig durchgeführt werden.
A.10.2.3	Management von Änderungen an Dienstleistungen durch Dritte	*Maßnahme* Änderungen an der Erbringung von Dienstleistungen, einschließlich des Aufrechterhaltens und Verbesserns der existierenden Sicherheitspolitik, Verfahren und Maßnahmen, müssen geregelt werden, und dies unter Berücksichtigung der Kritikalität der betroffenen Geschäftssysteme und -prozesse und einer zusätzlichen Risikobewertung.

A.10.3 – Systemplanung und -abnahme

A.10.3 Systemplanung und -abnahme *Ziel:* Minimierung des Risikos von Systemfehlern und Systemausfällen.		
A.10.3.1	Kapazitätsplanung	*Maßnahme* Die Verwendung der Ressourcen muss überwacht und abgestimmt werden und für zukünftige Kapazitätsanforderungen müssen Abschätzungen angestellt werden, um die geforderte Systemleistung sicherzustellen.
A.10.3.2	Systemabnahme	*Maßnahme* Für neue Informationssysteme, Upgrades und neue Versionen müssen Abnahmekriterien festgelegt werden und während der Entwicklung und vor der Abnahme müssen angemessene Systemtests durchgeführt werden.

A.10.4 – Schutz vor Schadsoftware und mobilem Programmcode

A.10.4 Schutz vor Schadsoftware und mobilem Programmcode *Ziel:* Schutz der Integrität von Software und Informationen.		
		Maßnahme

A.10.4.1	Maßnahmen gegen Schadsoftware	Maßnahmen zur Erkennung, Verhinderung und Wiederherstellung zum Schutz vor Schadsoftware sowie Maßnahmen und angemessene Verfahren zur Schärfung des Benutzerbewusstseins müssen umgesetzt werden.
A.10.4.2	Schutz vor mobiler Software (mobilen Agenten)	*Maßnahme* Wo die Verwendung von mobilen Programmcodes (mobile Agenten) genehmigt ist, muss die Konfiguration sicherstellen, dass diese mobilen Programmcodes gemäß einer klar definierten Sicherheitsrichtlinie betrieben werden und kein mobiler Programmcode ausgeführt wird, der nicht genehmigt wurde.
A.10.8.2	Vereinbarungen über den Austausch von Informationen	*Maßnahme* Vereinbarungen über den Austausch von Informationen zwischen der Organisation und Externen müssen getroffen werden.
A.10.8.3	Transport physischer Datenträger	*Maßnahme* Datenträger, die Informationen beinhalten, müssen während des Transports über Organisationsgrenzen hinweg vor unbefugten Zugriff, Missbrauch oder Verfälschung geschützt werden.
A.10.8.4	Elektronische Nachrichten (Messaging)	*Maßnahme* Informationen, die Teil einer elektronischen Nachrichtenübermittlung sind, müssen angemessen geschützt werden.
A.10.8.5	Geschäftsinformations-Systeme	*Maßnahme* Anweisungen und Verfahren müssen entwickelt und umgesetzt werden, um Informationen, die zwischen Geschäftsinformations-Systemen übertragen werden, zu schützen.

A.10.5 – Backup

A.10.5 Backup *Ziel:* Aufrechterhaltung der Integrität und der Verfügbarkeit von Informationen und informationsverarbeitenden Einrichtungen.		
		Maßnahme

A.10.5.1	Backup von Informationen	Backup-Kopien von Informationen und von Software müssen regelmäßig, im Einklang mit dem vereinbarten Backup-Verfahren, erstellt und getestet werden.

A.10.6 - Management der Netzsicherheit

A.10.6 Management der Netzsicherheit *Ziel:* Sicherstellung des Schutzes von Informationen in Netzen und der unterstützenden Infrastruktur.		
A.10.6.1	Maßnahmen für Netze	*Maßnahme* Um Netze vor Bedrohungen zu schützen, die Sicherheit von Systemen und Anwendungen in Netzen zu erhalten sowie die übertragenen Informationen zu schützen, müssen Netze angemessen verwaltet und kontrolliert werden.
A.10.6.2	Sicherheit von Netzdiensten	*Maßnahme* Sicherheitsmerkmale, Leistungsumfang und Administrationsanforderungen müssen für alle Netzdienste ermittelt und in eine Vereinbarung über Netzdienste aufgenommen werden, unabhängig davon, ob diese Dienste intern oder von externen Dienstleistern erbracht werden.

A.10.7 - Handhabung von Datenträgern

A.10.7 Handhabung von Datenträgern *Ziel:* Verhinderung unerlaubter Veröffentlichung, Veränderung, Entnahme oder Zerstörung von Vermögenswerten sowie Verhinderung der Unterbrechung des Geschäftsbetriebs.		
A.10.7.1	Verwaltung austauschbarer Datenträger	*Maßnahme* Es müssen Verfahren für den Umgang mit austauschbaren Datenträgern vorhanden sein.
A.10.7.2	Entsorgung von Datenträgern	*Maßnahme* Werden Datenträger nicht länger benötigt, müssen diese zuverlässig und sicher unter Anwendung formaler Verfahren entsorgt werden.
A.10.7.3	Umgang mit Informationen	*Maßnahme* Verfahren für den Umgang mit und der Speicherung von Information müssen etabliert

		werden, um diese Informationen vor unerlaubter Veröffentlichung oder Missbrauch zu schützen.
A.10.7.4	Sicherheit der Systemdokumentation	*Maßnahme* Die Systemdokumentation muss vor unbefugtem Zugriff geschützt werden.

A.10.8 - Austausch von Informationen

A.10.8 Austausch von Informationen *Ziel:* Die Erhaltung der Sicherheit von Informationen und Software, die innerhalb einer Organisation oder mit Externen ausgetauscht wird.		
A.10.8.1	Anweisungen und Verfahren zum Austausch von Informationen	*Maßnahme* Formale Anweisungen, Verfahren und Maßnahmen müssen vorhanden sein, um den Austausch von Informationen über alle Arten von Kommunikationseinrichtungen zu schützen.
A.10.10.3	Schutz von Protokollinformationen	*Maßnahme* Protokollierungseinrichtungen und Protokollinformationen müssen vor Verfälschung und unbefugtem Zugriff geschützt werden.
A.10.10.4	Administratorund Operatorprotokolle	*Maßnahme* Aktivitäten von Systemadministratoren und Systemoperatoren müssen protokolliert werden.
A.10.10.5	Fehlerprotokolle	*Maßnahme* Fehler müssen protokolliert und analysiert werden und es müssen entsprechende Maßnahmen ergriffen werden.
A.10.10.6	Zeitsynchronisation	*Maßnahme* Die Uhren aller wichtigen informationsverarbeitenden Systeme einer Organisation oder eines Sicherheitsbereichs müssen auf eine vereinbarte Referenzzeit synchronisiert werden.

A.10.9 – Anwendungen des elektronischen Geschäftsverkehrs

A.10.9 Anwendungen des elektronischen Geschäftsverkehrs

Ziel: Die Sicherheit und die sichere Benutzung von Anwendungen des elektronischen Geschäftsverkehrs.		
A.10.9.1	Elektronischer Geschäftsverkehr	*Maßnahme* Informationen für Anwendungen des elektronischen Geschäftsverkehrs, die über öffentliche Netze transportiert werden, müssen gegen betrügerische Aktivitäten, Vertragsstreitigkeiten, unberechtigte Veröffentlichung und Veränderung geschützt werden.
A.10.9.2	Online-Transaktionen	*Maßnahme* Informationen von Online-Transaktionen müssen geschützt werden, um unvollständige Übertragungen, falsches Routing, unbefugte Veränderung der Inhalte, unbefugte Offenlegung sowie unbefugte Vervielfältigung oder Replay-Angriffe zu verhindern.
A.10.9.3	Öffentlich zugängliche Informationen	*Maßnahme* Die Integrität von Informationen, die auf einem öffentlich zugänglichen System bereitgestellt werden, muss geschützt sein, um unbefugte Veränderung zu verhindern.

A.10.10 – Überwachung

A.10.10 Überwachung *Ziel:* Aufdeckung nicht genehmigter informationsverarbeitender Aktivitäten.		
A.10.10.1	Ereignisprotokolle	*Maßnahme* Es müssen Ereignisprotokolle erstellt werden, in denen Benutzeraktivitäten, ungewöhnliche Ereignisse und Informationssicherheitsvorfälle festgehalten werden. Sie müssen für einen vereinbarten Zeitraum verwahrt werden, um bei zukünftigen Untersuchungen und Überwachungen der Zugriffskontrolle behilflich zu sein.
A.10.10.2		*Maßnahme* Es müssen Verfahren zur Überwachung der Nutzung informationsverarbeitender Einrichtungen eingerichtet werden und die

	Überwachung der Systemnutzung	Ergebnisse der Überwachungen müssen regelmäßig überprüft werden.
A.10.10.3	Schutz von Protokollinformationen	*Maßnahme* Protokollierungseinrichtungen und Protokollinformationen müssen vor Verfälschung und unbefugtem Zugriff geschützt werden.
A.10.10.4	Administratorund Operatorprotokolle	*Maßnahme* Aktivitäten von Systemadministratoren und Systemoperatoren müssen protokolliert werden.
A.10.10.5	Fehlerprotokolle	*Maßnahme* Fehler müssen protokolliert und analysiert werden und es müssen entsprechende Maßnahmen ergriffen werden.
A.10.10.6	Zeitsynchronisation	*Maßnahme* Die Uhren aller wichtigen informationsverarbeitenden Systeme einer Organisation oder eines Sicherheitsbereichs müssen auf eine vereinbarte Referenzzeit synchronisiert werden.

A.11 – Zugriffskontrolle

A.11.1 - Geschäftliche Notwendigkeit der Zugriffskontrolle

A.11.1 Geschäftliche Notwendigkeit der Zugriffskontrolle *Ziel:* Kontrolle des Zugriffs auf Informationen.		
A.11.1.1	Zugriffskontroll-Politik	*Maßnahme* Eine Zugriffskontroll-Politik muss, basierend auf den Geschäftsund Sicherheitsanforderungen für Zugriffskontrollen, eingerichtet, dokumentiert und regelmäßig kontrolliert werden.

A.11.2 – Benutzerverwaltung

A.11.2 Benutzerverwaltung *Ziel:* Sicherstellung des Zugriffs auf Informationssysteme für Befugte und Verhinderung des Zugriffs auf Informationssysteme für Unbefugte.		
A.11.2.1	Benutzerregistrierung	*Maßnahme* Es muss für alle Informationssysteme und -dienste eine formale Benutzerregistrierung und -deregistrierung zur Vergabe und Rücknahme von Zugriffsberechtigungen geben.
A.11.2.2	Verwaltung von Sonderrechten	*Maßnahme* Die Zuweisung und Benutzung von Privilegien muss eingeschränkt und kontrolliert stattfinden.
A.11.2.3	Verwaltung von Benutzerpasswörtern	*Maßnahme* Die Zuweisung von Passwörtern muss durch einen formalen Managementprozess kontrolliert werden.
A.11.2.4	Überprüfung von Benutzerberechtigungen	*Maßnahme* Benutzerberechtigungen müssen regelmäßig, unter Anwendung eines formalen Prozesses, durch das Management überprüft werden.

A.11.3 - Verantwortlichkeiten der Benutzer

A.11.3 Verantwortlichkeiten der Benutzer *Ziel:* Verhinderung von unbefugtem Benutzerzugriff, Kompromittierung oder Diebstahl von Informationen und informationsverarbeitenden Einrichtungen.		
		Maßnahme

A.11.3.1	Passwortverwendung	Benutzer müssen aufgefordert werden, bei Auswahl und Anwendung von Passwörtern bewährten Sicherheitspraktiken zu folgen.
A.11.3.2	Unbeaufsichtigte Benutzergeräte	*Maßnahme* Benutzer müssen sicherstellen, dass unbeaufsichtigte Geräte ausreichend geschützt sind.
A.11.3.3	Arbeitsplatzordnung	*Maßnahme* Eine Anweisung bezüglich Aufräumens des Schreibtisches hinsichtlich Papiere und Datenträger sowie Löschen des Bildschirms von informationsverarbeitenden Einrichtungen muss eingeführt werden.

A.11.4 - Zugriffskontrolle für Netze

A.11.4 Zugriffskontrolle für Netze *Ziel:* Verhinderung von unbefugtem Zugriff auf Netzdienste.		
A.11.4.1	Anweisung zur Nutzung von Netzdiensten	*Maßnahme* Benutzer dürfen nur Zugriff auf solche Netzdienste bekommen, für deren Nutzung sie ausdrücklich berechtigt sind.
A.11.4.2	Benutzerauthentisierung für externe Verbindungen	*Maßnahme* Zur Kontrolle des Zugriffs von Benutzern mit Fernzugriff müssen angemessene Authentisierungsmaßnahmen getroffen werden.
A.11.4.3	Geräteidentifizierung in Netzen	*Maßnahme* Eine automatische Geräteidentifizierung muss als Mittel zur Authentisierung von Verbindungen von speziellen Orten und Geräten aus in Betracht gezogen werden.
A.11.4.4	Schutz der Diagnoseund Konfigurationsports	*Maßnahme* Der physische Zugang und der logische Zugriff auf Diagnoseund Konfigurationsports müssen einer Kontrolle unterliegen.
A.11.4.5	Trennung in Netzen	*Maßnahme*

		Gruppen von Informationsdiensten, Benutzern und Informationssystemen müssen in Netzen getrennt gehalten werden.
A.11.4.6	Kontrolle von Netzverbindungen	*Maßnahme* Für gemeinsame Netze, besonders für jene, die sich über die Grenzen einer Organisation hinaus erstrecken, muss die Fähigkeit der Benutzer, sich am Netz anzumelden, eingeschränkt sein. Diese Einschränkung muss im Einklang mit der Zugriffskontroll-Politik und den Anforderungen der Geschäftsanwendung (gemäß 11.1) stehen.
A.11.4.7	Routingkontrolle für Netze	*Maßnahme* Kontrollen für das Routing in Netzen müssen umgesetzt sein, um sicherzustellen, dass Computerverbindungen und Informationsflüsse nicht die Zugriffskontroll-Politik von Geschäftsanwendungen verletzen.

A.11.5 - Zugriffskontrolle auf Betriebssysteme

A.11.5 Zugriffskontrolle auf Betriebssysteme *Ziel:* Verhinderung von unbefugtem Zugriff auf Betriebssysteme.		
A.11.5.1	Verfahren für sichere Anmeldung	*Maßnahme* Der Zugriff auf Betriebssysteme muss durch ein sicheres Anmeldeverfahren kontrolliert werden.
A.11.5.2	Benutzeridentifizierung und Authentisierung	*Maßnahme* Alle Benutzer müssen eine eindeutige Benutzerkennung (User ID) für ihren persönlichen Gebrauch haben und eine geeignete Authentisierungstechnik muss eingesetzt werden, um die vorgegebene Identität des Benutzers zu bestätigen.
A.11.5.3	Systeme zur Verwaltung von Passwörtern	*Maßnahme* Systeme zur Verwaltung von Passwörtern müssen interaktiv sein und qualitative hochwertige Passwörter sicherstellen.
A.11.5.4		*Maßnahme* Die Verwendung von Dienstprogrammen, die in der Lage sind, sich über Systemund

	Verwendung von SystemDienstprogrammen	Anwendungseinstellungen hinwegzusetzen, muss eingeschränkt sein und genau kontrolliert werden.
A.11.5.5	Session Timeout	*Maßnahme* Inaktive Sessions müssen nach einer festgelegten Dauer Inaktivität geschlossen werden.
A.11.5.6	Begrenzung der Verbindungsdauer	*Maßnahme* Begrenzungen der Verbindungsdauer müssen verwendet werden, um zusätzliche Sicherheit für Anwendungen mit hohem Risiko zu schaffen.

A.11.6 - Zugriffskontrolle zu Anwendungen und Information

A.11.6 Zugriffskontrolle zu Anwendungen und Information *Ziel:* Verhinderung des unbefugten Zugriffs auf Informationen, die in Anwendungssystemen bereitgestellt werden.		
A.11.6.1	Einschränkung des Informationszugriffs	*Maßnahme* Der Zugriff auf Informationen und Funktionen eines Anwendungssystems durch Benutzer und Supportpersonal muss gemäß der festgelegten Zugriffskontroll-Politik eingeschränkt werden.
A.11.6.2	Isolierung sensibler Systeme	*Maßnahme* Sensible Systeme müssen sich in einem nur dafür bestimmten (isolierten) Rechnerumfeld befinden.

A.11.7 - Mobile Computing und Telearbeit

A.11.7 Mobile Computing und Telearbeit *Ziel:* Sicherstellung der Informationssicherheit bei der Benutzung von Einrichtungen für Mobile Computing und Telearbeit.		
A.11.7.1	Mobile Computing und Kommunikation	*Maßnahme* Um sich vor den Risiken bei der Verwendung von Mobile Computing und Kommunikationseinrichtungen zu schützen, muss eine formale Anweisung vorhanden und angemessene Maßnahmen getroffen worden sein.
A.11.7.2	Telearbeit	*Maßnahme*

		Anweisungen, Betriebspläne, und Verfahren für Telearbeit müssen entwickelt und implementiert werden.

A.12 - Beschaffung, Entwicklung und Wartung von Informationssystemen

A.12.1 - Sicherheitsanforderungen an Informationssysteme

A.12.1 Sicherheitsanforderungen an Informationssysteme *Ziel:* Sicherzustellen, dass Sicherheit ein integrierter Bestandteil in Informationssystemen ist.		
A.12.1.1	Analyse und Spezifikation der Sicherheitsanforderungen	*Maßnahme* In Vorgaben von Geschäftsanforderungen an neue Informationssysteme oder an Erweiterungen von bestehenden Informationssystemen müssen die Anforderungen an Sicherheitsmaßnahmen spezifiziert werden.

A.12.2 – Korrekte Verarbeitung in Anwendungen

A.12.2 Korrekte Verarbeitung in Anwendungen *Ziel:* Verhinderung von Fehlern, Verlust, unberechtigter Veränderung oder Missbrauch von Informationen in Anwendungen.		
A.12.2.1	Validierung von Eingabedaten	*Maßnahme* Daten, die in Anwendungen eingegeben werden, müssen validiert werden, um sicherzustellen, dass diese Eingaben korrekt und passend sind.
A.12.2.2	Kontrolle der internen Verarbeitung	*Maßnahme* Um Verfälschungen von Informationen durch Verarbeitungsfehler oder Vorsatz zu entdecken, müssen Validierungsprüfungen Bestandteil der Anwendung sein.
A.12.2.3	Integrität von Nachrichten	*Maßnahme* Anforderungen an die Sicherstellung von Authentizität und Integrität von Nachrichten in Anwendungen müssen identifiziert und entsprechende Maßnahmen müssen ausgewählt und umgesetzt werden.
A.12.2.4	Validierung von Ausgabedaten	*Maßnahme* Die Datenausgabe einer Anwendung muss validiert werden, um so sicherzustellen, dass die Verarbeitung der gespeicherten Informationen korrekt und den Umständen angemessen erfolgt ist.

A.12.3 - Kryptographische Maßnahmen

A.12.3 Kryptographische Maßnahmen *Ziel:* Schutz der Vertraulichkeit, Integrität und Authentizität von Informationen mittels Kryptographie.		
A.12.3.1	Anweisung zur Anwendung kryptographischer Maßnahmen	*Maßnahme* Eine Anweisung zur Anwendung kryptographischer Maßnahmen zum Schutz von Informationen muss entwickelt und umgesetzt werden.
A.12.3.2	Schlüsselverwaltung	*Maßnahme* Zur Unterstützung der Anwendung kryptographischer Techniken in einer Organisation muss eine Schlüsselverwaltung vorhanden sein.

A.12.4 - Sicherheit von Systemdateien

A.12.4 Sicherheit von Systemdateien *Ziel:* Die Sicherstellung der Sicherheit von Systemdateien.		
A.12.4.1	Maßnahmen für Software in Produktionssystemen	*Maßnahme* Um die Installation von Software in Produktionssystemen zu kontrollieren, müssen Verfahren vorhanden sein.
A.12.4.2	Schutz von Systemtest-Daten	*Maßnahme* Systemtest-Daten müssen sorgfältig ausgewählt, geschützt und kontrolliert werden.
A.12.4.3	Zugriffskontrolle zu ProgrammQuellcode	*Maßnahme* Der Zugriff auf den Programm-Quellcode muss eingeschränkt sein.

A.12.5 - Sicherheit bei Entwicklungs- und Supportprozessen

A.12.5 Sicherheit bei Entwicklungsund Supportprozessen *Ziel:* Aufrechterhaltung der Sicherheit von Anwendungssoftware und -informationen.		
A.12.5.1	Änderungskontroll-Verfahren	*Maßnahme* Die Umsetzung von Änderungen muss einem formellen Änderungskontroll-Verfahren unterliegen.

A.12.5.2	Technische Prüfung der Anwendungen nach Änderungen am Betriebssystem	*Maßnahme* Wenn Betriebssysteme geändert werden, müssen geschäftskritische Anwendungen überprüft und getestet werden, um sicherzustellen, dass es keine negative Auswirkungen auf den Betrieb und die Sicherheit der Organisation gibt.
A.12.5.3	Einschränkung von Änderungen an Softwarepaketen	*Maßnahme* Von Änderungen an Softwarepaketen muss abgeraten werden, diese müssen auf unentbehrliche Änderungen eingeschränkt werden und alle Änderungen müssen streng kontrolliert werden.
A.12.5.4	Durchsickern von Informationen	*Maßnahme* Gelegenheiten für ein Durchsickern von Informationen müssen verhindert werden.
A.12.5.5	Ausgelagerte Softwareentwicklung	*Maßnahme* Ausgelagerte Softwareentwicklung muss durch die Organisation beaufsichtigt und überwacht werden.

A.12.6 - Management technischer Schwachstellen

A.12.6 Management technischer Schwachstellen *Ziel:* Reduktion des Risikos der Ausnutzung von veröffentlichten technischen Schwachstellen.		
A.12.6.1	Maßnahmen in Bezug auf technische Schwachstellen	*Maßnahme* Informationen über technische Schwachstellen müssen rechtzeitig für die verwendeten Informationssysteme beschafft werden, die Gefährdung der Organisation gegenüber solcher Schwachstellen muss evaluiert werden und angemessene Maßnahmen müssen getroffen werden, um das damit verbundene Risiko abzudecken.

A.13 - Management von Informationssicherheits-Vorfällen

A.13.1 - Meldung von Informationssicherheits-Ereignissen und -Schwächen

A.13.1 Meldung von Informationssicherheits-Ereignissen und -Schwächen *Ziel:* Sicherstellung, dass Informationssicherheits-Ereignisse und Schwächen in Verbindung mit den Informationssystemen so kommuniziert werden, dass rechtzeitig korrigierende Aktionen getroffen werden können.		
A.13.1.1	Meldung von InformationssicherheitsEreignissen	*Maßnahme* Informationssicherheits-Ereignisse müssen so schnell wie möglich über die zuständigen Managementkanäle gemeldet werden.
A.13.1.2	Meldung von Sicherheitsschwächen	*Maßnahme* Alle Mitarbeiter*innen, Auftragnehmer*innen und Dritte als Anwender von Informationssystemen und -diensten müssen verpflichtet sein, alle beobachteten oder vermuteten Sicherheitsschwächen in Systemen oder Diensten festzuhalten und zu melden.

A.13.2 - Management von Informationssicherheits-Vorfällen und Verbesserungen

A.13.2 Management von Informationssicherheits-Vorfällen und Verbesserungen *Ziel:* Sicherstellung, dass ein einheitlicher und effektiver Ansatz für den Umgang mit InformationssicherheitsVorfällen angewendet wird.		
A.13.2.1	Verantwortlichkeiten und Verfahren	*Maßnahme* Management-Verantwortlichkeiten und Verfahren müssen eingerichtet werden, um eine schnelle, effektive und planmäßige Reaktion auf Informationssicherheits-Vorfälle sicherzustellen.
A.13.2.2	Lernen von InformationssicherheitsVorfällen	*Maßnahme* Es muss ein Mechanismus existieren, mit dem Art, Umfang und Kosten von Informationssicherheits-Vorfällen quantifiziert und überwacht werden kann.
A.13.2.3	Sammeln von Beweisen	*Maßnahme* Sofern aufgrund eines Informationssicherheits-Vorfalls rechtliche Schritte gegen eine Person oder Organisation ergriffen werden (entweder ziviloder strafrechtlich), müssen die gesammelten, aufbewahrten und vorgelegten

		Beweise die für die zuständige Gerichtsbarkeit erforderliche Beweisqualität aufweisen.

A.14 - Betriebliches Kontinuitätsmanagement (Business Continuity Management)

A.14.1 - Informationssicherheits-Aspekte des betrieblichen Kontinuitätsmanagements

A.14.1 Informationssicherheits-Aspekte des betrieblichen Kontinuitätsmanagements *Ziel*: Entgegenwirkung von Unterbrechungen bei Geschäftsaktivitäten und Schutz kritischer Geschäftsprozesse vor den Auswirkungen wesentlicher Störungen der Informationssysteme oder vor Katastrophen, sowie Sicherstellung der zeitnahen Wiederaufnahme der Geschäftstätigkeit.		
A.14.1.1	Einbeziehung von Informationssicherheit in den Management-Prozess des betrieblichen Kontinuitätsmanagements	*Maßnahme* Für die gesamte Organisation muss ein ManagementProzess zur Sicherstellung der betrieblichen Kontinuität entwickelt und aufrechterhalten werden, der die erforderlichen Informationssicherheits-Anforderungen an die betriebliche Kontinuität in der Organisation abdeckt.
A.14.1.2	Betriebliches Kontinuitätsmanagement und Risikobewertung	*Maßnahme* Ereignisse, die Unterbrechungen von Geschäftsprozessen verursachen können, müssen identifiziert werden, gemeinsam mit Wahrscheinlichkeit und Auswirkung solcher Unterbrechungen und deren Konsequenzen auf die Informationssicherheit.
A.14.1.3	Entwicklung und Umsetzung von Kontinuitätsplänen einschließlich der Informationssicherheit	*Maßnahme* Pläne müssen entwickelt und umgesetzt werden, um den Betrieb aufrechtzuerhalten oder wieder herzustellen und um die Verfügbarkeit von Informationen im erforderlichen Maß und im erforderlichen Zeitraum nach Unterbrechungen oder Ausfällen von kritischen Geschäftsprozessen sicherzustellen.
A.14.1.4	Rahmenwerk für die Planung der betrieblichen Kontinuität	*Maßnahme* Ein einheitliches Rahmenwerk für die Planung der betrieblichen Kontinuität muss aufrechterhalten werden, um so sicherzustellen, dass alle Pläne konsistent sind, um Informationssicherheits-Anforderungen einheitlich zu behandeln und um

		Prioritäten für Tests und Instandhaltung zu identifizieren.
A.14.1.5	Test, Instandhaltung und Neubewertung von Plänen der betrieblichen Kontinuität	*Maßnahme* Pläne zur betrieblichen Kontinuität müssen regelmäßig getestet und aktualisiert werden, um sicherzustellen, dass sie aktuell und effektiv sind.

A.15 - Einhaltung von Verpflichtungen

A.15.1 - Einhaltung gesetzlicher Verpflichtungen

A.15.1 Einhaltung gesetzlicher Verpflichtungen *Ziel:* Vermeidung von Verstößen gegen Gesetze, behördliche oder vertragliche Verpflichtungen und gegen jegliche Sicherheitsanforderungen.		
A.15.1.1	Identifizierung der anwendbaren Gesetze	*Maßnahme* Alle relevanten gesetzlichen, behördlichen und vertraglichen Anforderungen und der Ansatz der Organisation, diese Anforderungen zu erfüllen, müssen für jedes Informationssystem und die Organisation ausdrücklich definiert, dokumentiert und aktuell gehalten werden.
A.15.1.2	Rechte an geistigem Eigentum	*Maßnahme* Angemessene Verfahren müssen umgesetzt werden, um die Einhaltung gesetzlicher, behördlicher und vertraglicher Anforderungen für den Gebrauch von Material, für das geistige Eigentumsrechte bestehen könnte, und für die Nutzung von urheberrechtlich geschützten Softwareprodukten, sicherzustellen.
A.15.1.3	Schutz von organisationseigenen Aufzeichnungen	*Maßnahme* Wichtige Aufzeichnungen müssen im Einklang mit gesetzlichen, behördlichen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung und Fälschung geschützt werden.
A.15.1.4	Datenschutz und Geheimhaltung von personenbezogenen Informationen	*Maßnahme* Datenschutz und Geheimhaltung müssen gemäß den relevanten Gesetzen, Vorschriften und, falls anwendbar, Vertragsbestimmungen sichergestellt sein.
A.15.1.5	Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen	*Maßnahme* Benutzer müssen davon abgehalten werden, informationsverarbeitende Einrichtungen zu nicht genehmigten Zwecken zu benutzen.
	Regelungen von kryptographischen Maßnahmen	*Maßnahme*

A.15.1.6		Kryptographische Maßnahmen müssen im Einklang mit allen relevanten Vereinbarungen, Gesetzen und Vorschriften angewendet werden.

A.15.2 - Einhaltung von Sicherheitsanweisungen und -standards sowie technischer Vorgaben

A.15.2 Einhaltung von Sicherheitsanweisungen und -standards sowie technischer Vorgaben *Ziel:* Sicherstellung, dass Systeme die organisationsweiten Sicherheitsanweisungen und -standards einhalten.		
A.15.2.1	Einhaltung von Sicherheitsanweisungen und -standards	*Maßnahme* Manager müssen sicherstellen, dass alle Sicherheitsverfahren in ihrem Verantwortungsbereich korrekt angewendet werden, um die Einhaltung der Sicherheitsanweisungen und -standards zu erreichen.
A.15.2.2	Überprüfung der Einhaltung technischer Vorgaben	*Maßnahme* Informationssysteme müssen regelmäßig auf die Einhaltung von Standards zur Sicherheitsimplementierung überprüft werden.

A.15.3 - Überlegungen zu Audits von Informationssystemen

A.15.3 Überlegungen zu Audits von Informationssystemen *Zie*l: Maximierung der Effektivität und Minimierung der Störung der Informationssysteme im Zuge des Systemaudit-Prozesses.		
A.15.3.1	Maßnahmen für Audits von Informationssystemen	*Maßnahme* Auditanforderungen und -aktivitäten, die Prüfungen an im Betrieb befindlichen Systemen betreffen, müssen sorgfältig geplant und vereinbart werden, um das Risiko von Störungen der Geschäftsprozesse zu minimieren.
A.15.3.2	Schutz von Auditwerkzeugen für Informationssysteme	*Maßnahme* Der Zugriff auf Auditwerkzeuge für Informationssysteme muss geschützt werden, um jeden möglichen Missbrauch oder Kompromittierung zu verhindern.

Erklärungen:

[1] Erklärung: Der Begriff „Eigentümer*innen" bezeichnet eine natürliche oder juristische Person, welche die vom Management zugewiesene Verantwortung für die Kontrolle von Produktion, Entwicklung, Instandhaltung, Gebrauch und Sicherheit der Vermögenswerte hat. Der Begriff „Eigentümer*innen" bedeutet nicht, dass diese Person irgendwelche Eigentumsrechte an dem Wert hat.

[2] Erklärung: Der Begriff „Beschäftigung" wird hier benutzt, um die folgenden verschiedenen Situationen zu behandeln: vorübergehende oder längerfristige Beschäftigung von Personen, Zuweisung von Rollen, Änderung von Rollen, Zuweisung von Verpflichtungen und die Beendigung von Beschäftigungsverhältnissen.

Fragen zu ISMS

1. Welche Anweisungen zur Benutzung von Netzdiensten hat der Benutzer zu befolgen?
    a. **Antwort:** Benutzern darf der direkte Zugriff nur auf Dienste, deren Benutzung ihnen ausdrücklich gestattet wurde, erlaubt sein.

2. Ist die Kooperation zwischen Organisationen aufrechtzuhalten?
    a. **Antwort:** Entsprechende Kontakte zu Vollzugs- und Aufsichtsbehörden, Informationsdienstanbietern und Telekommunikationsbetreibern sind aufrechtzuerhalten.

3. Ist die Überprüfung und Bewertung der Informationssicherheitspolitik notwendig?
    a. **Antwort:** Ja, die Informationssicherheitspolitik ist regelmäßig und im Fall von Änderungen, die einen Einfluss auf sie haben könnten, auf ihre weitere Eignung zu überprüfen.

4. Welche Maßnahmen bei Zugriff auf Informationen sind zu treffen?
    a. **Antwort:** Die Anforderungen für Zugriffskontrollen sind zu definieren und zu dokumentieren. Der Zugriff ist entsprechend der Grundlage für Zugriffskontrollen zu beschränken.

5. Welche Maßnahme sind für Fachberatung und die erhaltenen Informationen zur Informationssicherheit vorzusehen?
    a. **Antwort:** Hausinterne oder spezialisierte (externe) Fachberater sind bei Fragen zur Informationssicherheit zu Rate zu ziehen und erhaltene Informationen in der gesamten Organisation weiterzuleiten.

6. Welche Maßnahmen sind bei der Benutzung von IKT-Systemen zu treffen?
    a. **Antwort:** Es sind Verfahren zur Überwachung der Benutzung von Einrichtungen der Informationsverarbeitung einzuführen, und das Ergebnis der Überwachungstätigkeit ist in regelmäßigen Abständen zu überprüfen.

7. Welche Maßnahmen sind beim Verwalten der Benutzerpasswörter zu treffen?
    a. **Antwort:** Die Zuweisung von Passwörtern ist durch einen formalen Managementprozess zu kontrollieren.

8. Welche Maßnahme kann den Verstoß gegen Sicherheitsanweisungen bewusster machen?
    a. **Antwort:** Verstöße von Mitarbeitern gegen die organisationseigenen Sicherheitsanweisungen und zugehörige Verfahren sind mit formalen Disziplinarverfahren zu ahnden.

9. Welche Maßnahmen erhöhen den richtigen Umgang mit Informationssicherheit?
    a. **Antwort:** Für alle Mitarbeiter der Organisation und im Bedarfsfall für Benutzer von Drittfirmen sind entsprechende Schulungen durchzuführen und regelmäßig aktualisierte Informationen zu Sicherheitspolitik und Verfahren der Organisation herauszugeben.

10. Welche Maßnahmen sind zur Effektivität der Kontrollverfahren anzuwenden?
    a. **Antwort:** Audits produktiver Systeme sind zu planen und zu vereinbaren, um das Risiko von Störungen und Unterbrechungen der Geschäftsprozesse zu minimieren.

11. Welche Maßnahmen sind beim LOGIN von Benutzern zu regeln?
    a. **Antwort:** Es ist ein formales Anmelde- und Abmeldeverfahren für Benutzer einzurichten, um den Zugriff auf alle Mehrbenutzerinformationssysteme und -dienste zu regeln

12. Welche Maßnahmen haben die Benutzer beim Passwortgebrauch zu befolgen?
    a. : **Antwort:** Benutzer haben bei der Wahl und beim Gebrauch von Passwörtern bewährte Sicherheitspraktiken zu befolgen.

13. Wie werden die Vermögenswerte festgestellt?
    a. **Antwort:** Ein Inventar aller wichtigen Vermögenswerte ist zu erstellen und laufend zu aktualisieren.

14. Welche Maßnahmen sind zur Erhaltung der Sicherheitspolitik zu treffen?
    a. **Antwort:** Das Management hat sicherzustellen, dass alle Sicherheitsverfahren innerhalb seines Zuständigkeitsbereiches korrekt ausgeführt werden und alle Bereiche innerhalb der Organisation einer regelmäßigen Überprüfung unterzogen werden, um die Einhaltung der Sicherheitsanweisungen und -normen sicherzustellen.

15. Welche Maßnahmen werden zur Identifizierung der Risiken beim Zugriff bzw. Zugang durch Dritte getroffen?
    a. **Antwort:** Die Risiken, die mit dem Zugriff bzw. Zugang zu organisationseigenen Einrichtungen der Informationsverarbeitung durch Dritte verknüpft sind, sind zu bewerten, und entsprechende Sicherheitskontrollen sind zu implementieren.

16. Wie wird die Einbeziehung der Sicherheit in die Arbeitsverantwortlichkeiten festgehalten?
    a. **Antwort:** Sicherheitsrollen und -verantwortlichkeiten wie in der Informationssicherheitspolitik der Organisation niedergelegt, sind, sofern zutreffend, in den Stellenbeschreibungen zu dokumentieren.

17. Ist die Kooperation zwischen Organisationen aufrechtzuhalten?
    a. **Antwort:** Entsprechende Kontakte zu Vollzugs- und Aufsichtsbehörden, Informationsdienstanbietern und Telekommunikationsbetreibern sind aufrechtzuerhalten.

18. Warum ist ein Managementforum für Informationssicherheit einzurichten?
    a. **Antwort:** Es ist ein Managementforum einzurichten, damit eine klare Richtungsvorgabe und sichtbare Unterstützung des Managements für Sicherheitsinitiativen sichergestellt ist.

19. Wie erfolgt die Überprüfung der Informationssicherheit (kein internes Audit)?
    a. **Antwort:** Die Implementierung der Informationssicherheitspolitik ist von unabhängigen Personen zu überprüfen.

20. Welche Anforderungen haben die Leitlinien für die Klassifizierung?
    a. **Antwort:** Klassifizierungen für Informationen und Kontrollmechanismen zum Schutz dieser Informationen sind gemäß den Geschäftsanforderungen für die gemeinsame oder beschränkte Nutzung von Informationen sowie gemäß den mit derartigen Anforderungen verbundenen geschäftlichen Folgen festzulegen.

21. Welche Maßnahmen sind für die Einhaltung anzuwendender Gesetze durchzuführen?
    a. **Antwort:** Für jedes Informationssystem sind alle anwendbaren gesetzlichen, behördlichen und vertraglichen Anforderungen genau zu definieren und zu dokumentieren.

22. Welche organisatorische Maßnahme erhöht die Verantwortung der Mitarbeiter?
    a. **Antwort:** In den Anstellungsbedingungen ist auf die Verantwortung des Mitarbeiters für die Informationssicherheit hinzuweisen.

23. Die Kennzeichnung und Handhabung von Informationen erfolgt auf welcher Grundlage?
    a. **Antwort:** Es sind Verfahren für die Kennzeichnung und Handhabung von Informationen gemäß der von der Organisation festgelegten Klassifizierung zu definieren.

24. Welche organisatorische Maßnahme erhöht die Vertraulichkeit von Informationen?
    a. **Antwort:** Von Mitarbeitern ist als Teil ihrer Anstellungsbedingungen eine Vertraulichkeitsvereinbarung zu unterschreiben.

25. Welche Maßnahmen sind bei sensiblen Systemen zu treffen?
    a. **Antwort:** Sensible Systeme sind in einem nur dafür bestimmten(isolierten) Rechnerumfeld aufzustellen.

26. Welches Schutzziel gehört nicht zur erweiterten CIA – Triade
    a. **Antwort:** Paritätskontrolle
        i. Die Paritätskontrolle dient der Erkennung fehlerhaft übertragener Informationswörter. Als Informationswort wird hier eine Folge von Bits bezeichnet. Die „Parität" bezeichnet die Anzahl der mit 1 belegten Bits im Informationswort und heißt gerade (engl. „even"), wenn die Anzahl dieser Bits gerade ist, andernfalls ungerade (engl. „odd"). Die

Paritätskontrollcodierung hängt dem Informationswort ein Paritätskontrollbit, auch Paritybit genannt, an. Dies geschieht so, dass alle zu übertragenden Codewörter die gleiche Parität haben.

27. Welches Schutzziel gehört zur erweiterten CIA – Triade
    a. **Antwort: Nichtabstreitbarkeit = Non-Repudiation**

28. Welche Maßnahmen sind bei Ferndiagnoseport zu treffen?
    a. **Antwort:** Der Zugang zu Diagnoseports ist sicher zu kontrollieren.

29. Welche Maßnahmen sind in der Topologie von Netzwerken zu treffen?
    a. **Antwort**: In Netzwerken sind Kontrollen zur Trennung der Informationsdienste, Benutzergruppen und Informationssysteme zu treffen.

30. Welche Maßnahmen sind bei Rechenuhren (Systemzeit) zu treffen?
    a. **Antwort**: Rechenuhren sind zu synchronisieren, um exakte Aufzeichnungen sicherzustellen.

31. Welche Maßnahmen sind für die Benutzeridentifikation und -authentisierung zu treffen?
    a. **Antwort**: Allen Benutzern ist eine eindeutige Kennung (User-ID) für ihren persönlichen und alleinigen Gebrauch zuzuweisen, damit Aktivitäten auf die verantwortliche Person zurückgeführt werden können. Eine angemessene Authentisierungstechnik muss gewählt werden, um die vorgegebene Identität des Benutzers zu belegen.

32. Welche Maßnahmen sind mit Ereignisprotokollen zu treffen?
    a. **Antwort**: Auditprotokolle, in denen Ausnahmefälle und andere sicherheitsrelevante Vorfälle verzeichnet werden, sind zu erstellen und über einen vereinbarten Zeitpunkt aufzubewahren, um zukünftige Ermittlungen und die Überwachung der Zugriffskontrolle zu unterstützen.

33. Welche Maßnahmen haben die Benutzer bei unbeaufsichtigten Benutzergeräten sicherzustellen?
    a. **Antwort**: Benutzer haben sicherzustellen, dass unbeaufsichtigte Anlagen und Geräte entsprechend geschützt sind.

34. Welche Maßnahmen sind beim Routing im Netzwerk zu treffen?
    a. **Antwort**: Für gemeinsame Netze sind Routing-Kontrollen vorzusehen, um sicherzustellen, dass Rechnerverbindungen und Informationsflüsse nicht gegen die Zugangskontrollanweisungen für Geschäftsanwendungen gemäß den Anforderungen der Zugriffskontroll-Politik verstoßen.

35. Welche Maßnahme kann die Bewertung von Vorfällen erleichtern?
    a. **Antwort**: Es sind Verfahren einzurichten, mit denen Art, Häufigkeit und Kosten von Vorfällen und Fehlfunktionen quantifiziert und überwacht werden können.

36. Welche Maßnahmen sind bei Telearbeit zu treffen?
    a. **Antwort:** Grundlagen und Verfahren zur Genehmigung und Kontrolle der Telearbeit sind zu entwickeln.

37. Welche Maßnahmen sind zum Schutz geistigen Eigentums zu treffen?
    a. **Antwort:** Geeignete Verfahren, welche die Übereinstimmung mit rechtlichen Einschränkungen über die Nutzung von Material in Bezug auf den Schutz geistigen Eigentums und den Gebrauch gesetzlich oder patentrechtlich geschützter Softwareprodukte sicherstellen, sind zu implementieren.

38. Welche Maßnahmen sind bei der Verwaltung von Privilegien zu treffen?
    a. **Antwort**: Die Zuweisung und Benutzung von Privilegien ist zu beschränken und zu überwachen.

39. Welche Maßnahmen für Einrichtungen der Informationsverarbeitung muss eingeführt werden?
    a. **Antwort**: Ein Prozess zur Autorisierung neuer Einrichtungen der Informationsverarbeitung durch Geschäftsführung muss eingeführt werden.

40. Welche Maßnahmen beim Überprüfen der Zugriffsrechte von Benutzern sind zu treffen?
    a. **Antwort**: Zur Überprüfung der Zugriffsrechte für Benutzer ist in regelmäßigen Abständen ein formaler Prozess durchzuführen

41. Warum und aus welchen Personen ist in großen Organisationen ein Forum zur Koordination der Informationssicherheit einzurichten?
    a. **Antwort**: In großen Organisationen ist ein bereichsübergreifendes Forum einzurichten, das sich aus Vertretern des Managements der relevanten Bereiche der Organisation zusammensetzt und über das die Implementierung von Kontrollen der Informationssicherheit koordiniert wird.

42. Welche Maßnahmen sind beim Einsatz von portablen Computern zu treffen?
    a. **Antwort**: Zum Schutz vor Risiken, die beim Einsatz portabler Computer, insbesondere in ungeschützten Umgebungen, entstehen, sind formale Grundlagen zu etablieren und entsprechende Kontrollen zu schaffen.

43. Personenüberprüfungen und Personalpolitik sind wann durchzuführen?
    a. **Antwort**: Überprüfungen bei fest anzustellenden Mitarbeitern, Auftragnehmern und vorübergehend Beschäftigten sind zum Zeitpunkt der Bewerbung durchzuführen.

44. Welche Maßnahme ist bei Softwarefehlern notwendig?
    a. **Antwort**: Zur Meldung von Softwarefehlern sind entsprechende Verfahren einzurichten.

45. Welche Maßnahme ist bei Sicherheitsvorfällen notwendig?
    a. **Antwort**: Sicherheitsvorfälle sind unverzüglich nach Entdeckung des Vorfalls über entsprechende Managementkanäle zu melden.

46. Welche Maßnahme ist bei Sicherheitsschwachstellen notwendig?
    a. **Antwort**: Benutzer von Informationsdiensten haben alle beobachteten oder vermuteten Sicherheitsschwachstellen oder Bedrohungen der Systeme oder Dienste aufzuzeichnen und zu melden.

47. Welche Maßnahmen sind bei der Verwaltung von Passwörtern zu treffen?
    a. **Antwort**: Ein Passwortverwaltungssystem hat als effektive, interaktive Einrichtung vorzuliegen, durch die qualitativ hochwertige Passwörter sichergestellt werden.

48. Welche Maßnahmen sind beim Gebrauch von Systemdienstprogrammen zu treffen?
    a. **Antwort**: Die Benutzung von Systemdienstprogrammen ist zu beschränken und genau zu überwachen.

49. Welche Maßnahmen sind zur Sicherheit der Netzdienste zu treffen?
    a. **Antwort**: Es ist eine klare Beschreibung der Sicherheitsattribute aller von der Organisation benutzten Netzdienste vorzulegen.

50. Wer hat die Informationssicherheitspolitik zu veröffentlichen?
    a. **Antwort**: Von der Geschäftsführung ist ein Dokument zur Informationssicherheitspolitik zu genehmigen, zu veröffentlichen und allen Mitarbeitern nach Bedarf zur Kenntnis zu bringen.