KISTERS

Klassifikation der Informationswerte - Zutritts-, Zugangs- und Zugriffskontrolle

v.5.7, 2025-09-22

Verantwortlich:

KISTERS CISO

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation und Ziele

Zur Erreichung und Erhaltung der Informationssicherheit müssen Maßnahmen ergriffen werden, die eine unberechtigte oder missbräuchliche Nutzung von Unternehmenswerten verhindern. Zu den Unternehmenswerten gehören alle Gebäude, IT-Systeme, Anwendungen und alle Daten und Informationen, die betrieblich genutzt werden und wichtig oder sogar kritisch für den erfolgreichen Geschäftsbetrieb sind.
In dieser Richtlinie werden konkrete Maßnahmen zum Umgang mit Unternehmenswerten sowie dem Management von Zutritts-, Zugangs- und Zugriffsberechtigungen vorgegeben. Die Zutrittskontrolle betrifft den physischen Zutritt zu Gebäuden, Räumen und IT-Systemen, die Zugangskontrolle betrifft die Nutzung der IT-Systeme, die Zugriffskontrolle betrifft den Zugriff auf jegliche Daten, Information und Dokumente entsprechend ihrer Kritikalität und Klassifizierung.

1.2 Anwendungsbereich

Diese Richtlinie gilt für die gesamte KISTERS Gruppe sowie externe Dritte, die Zutritt zu KISTERS Gebäuden, Zugang zu KISTERS IT-Systemen oder den Zugriff auf KISTERS Daten benötigen. Sie ist Bestandteil der „KISTERS Informationssicherheitsrichtlinie“ [1]. Verbindlichkeit, Terminologie, Ansprechpartner und weitere Informationen gelten entsprechend.

1.3 Rollen, Verantwortlichkeiten und Abhängigkeiten

Die Verantwortlichkeiten für die in dieser Richtlinie beschriebenen Tätigkeiten sind in der folgenden Tabelle nach dem RACI-Prinzip dargestellt. Soweit erforderlich sind die Rollen in der „KISTERS IS Organisation“ [2] definiert.

	ISMT	System-verant-wortliche (1)	Teamlei-ter / Vor-gesetzte	Kontakt-personen für ex-terne Dritte	Mitarbei-ter	Externe Dritte	IT Admi-nistration
Definition System und Informationsklassifikation und Maßnahmen	A/R	I	I	I	I	I	I
Klassifikation von Werten	C	A/R	I	I	I		I
Beantragung (Einrichtung/Entzug) von Zutritts-, Zugangs-, Zugriffsrechten		C	A/R	A/R (2)	R (3)	R (2)	I
Genehmigung (Einrichtung/Entzug) von Zutritts-, Zugangs-, Zugriffsrechten		A/R	A/R (3)	C	I	I	I
Einrichtung/Entzug von Zutritts-, Zugangs-, Zugriffsrechten	C	A/R	C	C	I	I	C
Einrichtung Benutzerkonten (IT-Systeme)	I	A	C	C	I	I	R

	ISMT	System-verant-wortliche (1)	Teamlei-ter / Vor-gesetzte	Kontakt-personen für ex-terne Dritte	Mitarbei-ter	Externe Dritte	IT Admi-nistration
Überprüfung von Zu-tritts-, Zugangs-, Zu-griffsrechten	I	A/R	C	C			I

(1): allgemein: Verantwortliche für die betroffenen Unternehmenswerte (Standorte, Gebäude, IT-Systeme, Informationen)
(2): bei Rechtevergabe für externe Dritte (Kunden, Partner, Dienstleister etc.)
(3): Mitarbeiter können selbstständig Rechte beantragen; in dem Fall erfolgt die Genehmigung durch die Teamleiter / Vorgesetzten

1.4 Anwendbare rechtliche und regulatorische Anforderungen

Die Klassifikation von Werten sowie die Kontrolle von Zutritt, Zugang und Zugriff ist eine Grundvoraussetzung für die Einhaltung von ISO 27001, SOC 2, BSI C5 und anderen Informationssicherheitsstandards [3]. In individuellen Verträgen mit Kunden hat sich KISTERS verpflichtet, die Einhaltung eines oder mehrerer dieser Sicherheitsstandards oder gleichwertiger individueller Kundenanforderungen zu gewährleisten und aufrechtzuerhalten. Der Zugang zu kundenspezifischen Systemen und Zugriff auf kundenbezogene Informationen ist individuell vertraglich durch Geheimhaltungs- oder Vertraulichkeitsvereinbarungen geregelt. Spezifisch für den Zugriff auf personenbezogene Daten sind darüber hinaus die einschlägigen Datenschutzvorschriften [3] zu beachten.

2 Autorisierung/Rechtevergabe

Der Zutritt zu Gebäuden und Räumen, der Zugang zu IT-Systemen und der Zugriff auf Informationen und Geschäftsprozesse der KISTERS Gruppe MUSS immer auf Basis von Geschäfts- und Sicherheitsanforderungen autorisiert und kontrolliert werden. Autorisierungen KÖNNEN personen- oder gruppenbezogen definiert und erteilt werden.
Alle Rechte MÜSSEN nach dem Prinzip der „minimalen Rechtevergabe“ („principle of least privilege“) und dem Prinzip „Kenntnis nur bei Bedarf“ („minimum need to know principle“) vergeben werden. Die Verantwortlichen MÜSSEN die vergebenen Rechte regelmäßig überprüfen.

2.1 Privilegierte Zutritts-, Zugangs- und Zugriffsrechte

[INFO] Privilegierte Zutritts-, Zugangs- und Zugriffsberechtigungen sind solche, die Aktivitäten ermöglichen, die die Vertraulichkeit, Integrität oder Verfügbarkeit von produktiven Daten in intern genutzten IT-Systemen oder KISTERScloud-Systemen beeinträchtigen können. Dazu gehören Aktivitäten wie

- physische Änderungen der betrieblichen und/oder sicherheitstechnischen Komponenten von IT-Systemen von produktiven Systemen, z.B. das Ein- und Ausschalten von IT-Systemen, Austausch von Hardware, Modifikation von Netzwerkverkabelung, Abschalten von Sicherheitsvorrichtungen etc.;

- Änderungen an der betrieblichen und/oder sicherheitstechnischen Konfiguration der Systemkomponenten von produktiven Systemen, insbesondere das Starten, Stoppen, Löschen oder Deaktivieren von Systemkomponenten, auch mittelbar, z.B. durch Deaktivieren der Protokollierung und Überwachung sicherheitsrelevanter Ereignisse, Abschaltung von Virenscannern etc.;
- lesender oder schreibender Zugriff auf vertrauliche verarbeitete, gespeicherte oder übertragene Daten (KISTERS Daten, Kundendaten), soweit diese Daten nicht verschlüsselt sind oder die Verschlüsselung für den Zugriff aufgehoben werden kann.

Für privilegierte Berechtigungen müssen folgende Vorgaben eingehalten werden:

- Privilegierte Berechtigungen MÜSSEN personalisiert und restriktiv nach dem „Need-to-Know-Prinzip“ zugewiesen werden.
- Die Vergabe von privilegierten Berechtigungen MUSS vom Vorgesetzten / Teamleiter und dem Systemverantwortlichen genehmigt werden.
- Sofern die Berechtigungen nicht zur Erfüllung der gewöhnlichen Aufgaben eines Mitarbeiters notwendig sind, SOLLEN diese Berechtigungen gemäß einer Risikobewertung zeitlich befristet vergeben werden.
- Privilegierte Berechtigungen MÜSSEN bei Rollenwechsel oder Ausscheiden von Mitarbeitern unverzüglich entzogen werden, wenn möglich innerhalb von 24 Stunden.
- Die Aktivitäten von Benutzern mit privilegierten Berechtigungen SOLLEN soweit technisch möglich protokolliert werden, um einen Missbrauch dieser Berechtigungen im Verdachtsfall aufdecken zu können.
- Die protokollierten Informationen SOLLEN soweit technisch möglich automatisch auf Ereignisse überwacht werden, die einen Missbrauch darstellen können.
- Bei Identifikation eines solchen Ereignisses MÜSSEN die Verantwortlichen informiert werden, um unverzüglich beurteilen zu können, ob ein Missbrauch vorliegt und entsprechende Maßnahmen einzuleiten sind.

2.2 Verantwortliche

[INFO] Die Verantwortung für die Zuteilung von Zutritts-, Zugangs- und Zugriffsrechten wird im Allgemeinen durch ein Vier-Augen-Prinzip geregelt („segregation of duties“). Dies sind einerseits der für den Unternehmenswert verantwortliche Mitarbeiter (Systemverantwortliche) und andererseits der für die betroffene Person oder Gruppe verantwortliche Mitarbeiter (Teamleiter / Vorgesetzte bzw. Mitarbeiter, die Kontaktpersonen für Externe Dritte sind).

2.2.1 Systemverantwortliche

Für jedes Gebäude, jedes IT-System, jede Anwendung und jede Information MÜSSEN ein oder mehrere KISTERS Mitarbeiter als Verantwortliche benannt werden, die für die Klassifikation dieser Unternehmenswerte sowie für die Erteilung von Nutzungsrechten (Autorisierung) in Form von Zutritts-, Zugangs- und Zugriffsrechten innerhalb des Systems verantwortlich sind (operative Funktion)
Sofern kein anderer Verantwortlicher benannt wurde, ist der Urheber/Ersteller oder Eigentümer des Firmenwertes für die Klassifikation und für die Vergabe und Kontrolle der Autorisierungen verantwortlich.

2.2.2 Teamleiter / Vorgesetzte

Die Beantragung von Gewährung und Widerruf von Autorisierungen für KISTERS Mitarbeiter MUSS von einem vorgesetzten Teamleiter oder einem Vertreter durchgeführt werden.
Bei der Einstellung neuer Mitarbeiter MUSS der Vorgesetzte alle für den neuen Mitarbeiter notwendigen Zutritts-, Zugangs- und Zugriffsrechte beantragen. Beim Ausscheiden oder der Änderung der Rolle eines Mitarbeiters MUSS der Vorgesetzte sofort die Verantwortlichen für die vom Mitarbeiter genutzten Gebäude, IT-Systeme und Informationen informieren und eine Prüfung und ggfs. Änderung der Autorisierung veranlassen (kontrollierende Funktion).
Detaillierte Regelungen zu diesen Prozessen sind in der Richtlinie „KISTERS Personalmanagement“ [4] festgehalten.

2.2.3 Kontaktpersonen für Externe Dritte

Die Gewährung und der Widerruf von Autorisierungen für Externe MÜSSEN von KISTERS Mitarbeitern beantragt werden, die als Ansprechpartner oder Koordinatoren für die Zusammenarbeit mit diesen Externen Dritten verantwortlich sind. Kontaktpersonen sind je nach konkretem Fall

- Projektleiter, z.B. für Kunden oder Partner,
- Fach- oder Systemverantwortliche, z.B. bei externen Dienstleistern,
- andere autorisierte Mitarbeiter als Ansprechpartner oder Koordinatoren.

Die Kontaktpersonen MÜSSEN die Notwendigkeit und den aktuellen Stand der Autorisierungen für die von ihnen betreuten Externen regelmäßig überprüfen und ggfs. die Änderung oder Löschung von Autorisierungen veranlassen (kontrollierende Funktion). Dies gilt insbesondere bei der Beendigung von Projekten, Kooperationen, Partnerschaften oder Kundenverhältnissen.

2.2.4 Standortleiter

An jedem Standort KÖNNEN durch den Standortleiter spezielle Regelungen getroffen werden, solange sie nicht den in diesem Dokument beschriebenen allgemeinen Maßnahmen widersprechen. Standortleiter KÖNNEN ebenfalls im Einvernehmen mit dem CISO Ausnahmen von den allgemeinen Regelungen genehmigen, sofern die Umsetzung der allgemeinen Regelungen technisch nicht möglich oder wirtschaftlich unangemessen ist. Bei signifikanten Abweichungen MUSS eine Risikobewertung vorgenommen werden.

2.3 Genehmigung

Bevor Zutritts-, Zugangs- und Zugriffsrechte vergeben oder geändert werden, MUSS dies genehmigt werden, sowohl durch den Teamleiter/Vorgesetzten bzw. die Kontaktperson für externe Dritte als auch durch den Systemverantwortlichen genehmigt werden (Vier-Augen-Prinzip). Der Genehmigungsprozess läuft dabei in den folgenden Schritten ab:

- Bei Beantragung der Einrichtung oder Änderung von Zutritts-, Zugangs- oder Zugriffsrechten von Mitarbeitern oder Externen Dritten selbst MUSS der Vorgesetzte bzw. der Verantwortliche für die Externen Dritten die Einrichtung oder Änderung genehmigen.
- Bei Beantragung oder nach Genehmigung der Einrichtung oder Änderung von Zutritts-, Zugangs- oder Zugriffsrechten durch den Vorgesetzten bzw. Verantwortlichen für die Externen Dritten MUSS der Systemverantwortliche die Anforderung überprüfen und freigeben.

2.4 Dokumentation

Die Vergabe von Zutritts-, Zugangs- und Zugriffsrechten MUSS für Revisionszwecke geeignet protokolliert werden. Geeignete Möglichkeiten zur Protokollierung sind

- Tickets im KISTERS Ticketsystem,
- Eintragung in Gruppenlisten von IT-Systemen oder Anwendungen, soweit sich die Berechtigung der Autorisierung eines Mitarbeiters oder Externen aus seiner Rolle oder Aufgabenbeschreibung ergibt,
- Übergabelisten oder Übergabeprotokolle von Betriebsmitteln, die den Zutritt, Zugang oder Zugriff auf Unternehmenswerte ermöglichen (Firmenausweis, Schlüssel, Passwörter, etc.),
- Eintragung in Verteilerlisten von Dokumenten,
- gesonderte schriftliche oder elektronische Protokolle, sofern eine explizite Begründung für die Gewährung der Rechte erforderlich oder sinnvoll ist.

2.5 Überprüfung

Die Gültigkeit und Notwendigkeit der vergebenen Zutritts-, Zugangs- und Zugriffsrechte MUSS regelmäßig bzw. anlassbezogen durch die Verantwortlichen überprüft werden. Jede durchgeführte Überprüfung und daraus resultierende Maßnahmen MÜSSEN für Revisionszwecke geeignet protokolliert werden. Die regelmäßige Überprüfung KANN stichprobenartig durchgeführt werden, sofern es sich nicht um privilegierte Zutritts-, Zugangs- oder Zugriffsrechte handelt. Privilegierte Berechtigungen SOLLEN regelmäßig vollständig überprüft werden.
Die Zyklen für die Überprüfung SOLLEN dem Schutzbedarf der Unternehmenswerte und dem Aufwand der Überprüfung angemessen sein.
Eine anlassbezogene Überprüfung und entsprechende Anpassung der eingeräumten Zutritts-, Zugangs- und Zugriffsrechte MUSS in jedem Fall erfolgen, wenn sich die vertragliche Grundlage für die Einräumung von Rechten ändert, z.B. auf der Grundlage der

- Änderung / Beendigung des Arbeitsverhältnisses von KISTERS-Mitarbeitern oder externen Nutzern,
- Änderung / Beendigung des Vertragsverhältnisses mit Kunden oder Partnern,
- Änderung der rechtlichen Grundlagen für die Nutzung von Systemen oder Informationen.

Eine anlassbezogene Prüfung MUSS umgehend erfolgen, sofern der Mitarbeiter über privilegierte Zutritts-, Zugangs- oder Zugriffsberechtigungen verfügt.
Bei der Überprüfung festgestellte Abweichungen SOLLEN spätestens 7 Arbeitstage nach ihrer Feststellung durch Ändern oder Entziehen der Berechtigungen behandelt werden. Bei einer Änderung des Aufgabengebietes SOLLEN privilegierte Zutritts-, Zugangs- und Zugriffsberechtigungen innerhalb von 48h und andere Zutritts-, Zugangs- und Zugriffsberechtigungen innerhalb von 7 Arbeitstagen nach Inkrafttreten der Änderung entzogen werden.

2.6 Personengruppen

Folgende Personengruppen MÜSSEN im Allgemeinen bei der Vergabe von Zutritts-, Zugangs- und Zugriffsberechtigungen unterschieden werden:

	Personengruppe	**Beschreibung / Beispiele**
G0	Öffentlichkeit	• jeder

	Personengruppe	Beschreibung / Beispiele
G1	Externe Partner	• Besucher • Kunden, Partner • Auftragnehmer, Dienstleister, Lieferanten
G2	Mitarbeiter	• Mitarbeiter der KISTERS Gruppe • Praktikanten, Aushilfen • Dienstleister, Unterauftragnehmer mit Sondergenehmigung
G3	Autorisierte Mitarbeiter Autorisierte Externe	• Mitarbeiter oder Externe mit Autorisierung für definierte Bereiche, Systeme oder Informationen
G4	Speziell autorisierte Mitarbeiter	• Mitarbeiter mit Autorisierung für definierte Bereiche, Systeme oder Informationen mit besonderem Schutzbedarf

Falls notwendig KÖNNEN zusätzlich zu dieser Klassifizierung weitere Personengruppen für die Autorisierung und Rechtevergabe definiert werden.

2.7 Verbot der Missachtung

Mitarbeiter und Externe DÜRFEN NICHT vorsätzlich oder grob fahrlässig die vorgegebenen Maßnahmen zur Zutritts-, Zugangs- und Zugriffskontrolle umgehen oder ignorieren.
[INFO] Der nicht-autorisierte Zutritt, Zugang oder Zugriff auf Unternehmenswerte, z.B. durch Einbruch, Diebstahl, Hacking, Passwortmissbrauch, Erschleichung von Rechten oder andere Aktionen, wird im Rahmen der gesetzlichen Möglichkeiten arbeitsrechtlich und strafrechtlich und verfolgt.

3 Zutrittskontrolle

[INFO] Das Management von Zutrittskontrollen erfordert eine Klassifikation aller KISTERS Gebäude und Betriebsstätten in Sicherheitszonen auf Basis ihres Schutzbedarfs.
Für jeden KISTERS Standort MÜSSEN Gebäude, Gebäudeteile und Diensträume von der lokalen Standortleitung bzw. den Lokalen Information Security Officers (LISOs) den Sicherheitszonen zugeordnet werden.
Für jede Sicherheitszone MÜSSEN adäquate Maßnahmen für die Kontrolle und Überwachung des physikalischen Zutritts festgelegt werden. Alle Mitarbeiter der KISTERS Gruppe MÜSSEN über die Maßnahmen informiert werden und erhalten eine Einführung zu den standort-spezifischen Sicherheitszonen vor Ort.

3.1 Sicherheitszonen

Für die Zutrittsregelung von Betriebsstätten (Gebäuden, Gebäudeteilen und Räumen) der KISTERS Gruppe gilt folgende Klassifikation nach Sicherheitszonen:

	Sicherheitszone	Beschreibung / Beispiele
Z0	Außenbereiche	• Öffentliche Wege und Straßen • Nachbargrundstücke • Öffentlich zugängliche Zufahrten, Parkplätze und Parkhäuser • Flure, Treppenhäuser, Tiefgaragen in Gebäuden, die nicht ausschließlich von KISTERS genutzt werden
Z1	Kontrollierte Innenbereiche	• Gebäudeteile oder Räume für Publikumsverkehr, die einen von Internen Bereichen unabhängigen Zugang haben • Rezeption, Empfangsräume

	Sicherheitszone	Beschreibung / Beispiele
		• Schulungs-, Besprechungs-, Demoräume ohne Zugänge zu Internen Bereichen • Bereiche für Waren-Anlieferung und –Abholung • Casino (AC, OL)
Z2	Interne Bereiche	• Alle Gebäude und Gebäudeteile, die ausschließlich von KISTERS genutzt werden • Büroräume, interne Besprechungsräume, Lager, Flure • Schulungs-, Besprechungs-, Demo-Räume ohne unabhängigen Zugang
Z3	Sicherheitsbereiche	• Alle Gebäudeteile und Räume mit besonderem Schutzbedarf • Technikräume, Serverräume • Räume mit SMGWA-Arbeitsplätzen (auch bei Kunden) [8] • Büroräume, Aktenlager und Archive mit hohem Schutzbedarf wegen Datenschutz (z.B. Personaldaten)
Z4	Hochsicherheitsbereiche	• Rechenzentrum (AC)

[INFO] Standortspezifische Gegebenheiten oder Regelungen, soweit in dieser Richtlinie erfasst, sind explizit gekennzeichnet: (AC): Standort Aachen, (OL): Standort Oldenburg.

3.2 Zutrittsberechtigungen

Die Zutrittsberechtigungen der Personengruppen zu den Sicherheitszonen sind in der folgenden Tabelle zusammengefasst:

\Gruppe Zone	**G0 (jeder)**	**G1 (Externe)**	**G2 (KISTERS)**	**G3 (Autorisierte)**	**G4 (Spez. Aut.)**
Z0 (außen)	X	X	X	X	X
Z1 (kontrolliert)	-	X	X	X	X
Z2 (innen)	-	1,4	X	X	X
Z3 (sicher)	-	2,4	2,4	2,3,4	2,3,4
Z4 (hochsicher)	-	2	2	2	2,3

-: kein Zutritt

X: uneingeschränkter Zutritt

1: Zutritt nur in Begleitung eines KISTERS Mitarbeiters

2: Zutritt nur in Begleitung einer für den jeweiligen Bereich autorisierten Person

3: Zutritt ohne Begleitung, mit Autorisierung für den jeweiligen Bereich

4: Zutritt ohne Begleitung nur mit expliziter Zutrittserlaubnis durch den KISTERS Vorstand oder einen autorisierten Vertreter, z.B. die Standortleitung

3.3 Maßnahmen zur Zutrittskontrolle und Überwachung

Für die oben beschriebenen Sicherheitszonen gelten die im Folgenden aufgeführten Kontroll- und Überwachungsmaßnahmen für den physikalischen Zutritt.

3.3.1 Außenbereiche (Z0)

Maßnahme	Umsetzung	Bemerkungen
Überwachung	Überwachung SOLL durch Videokameras erfolgen, speziell an Gebäudeeingängen.	Soweit am Standort vorhanden.
Verhalten	Verdächtige Aktivitäten MÜSSEN am Empfang gemeldet und weiter durch die Rezeptionisten beobachtet werden.	

3.3.2 Kontrollierte Innenbereiche (Z1)

Maßnahme	Umsetzung	Bemerkungen
Sicherung	Außerhalb der für jeden Standort festgelegten Geschäftszeiten MUSS der Bereich gegen unbefugten Zutritt von außen verschlossen sein.	Mindestanforderung
Sicherung	Der Zutritt DARF NUR über ein Aufschließen über geeigneten Schlüssel (Firmenausweis, mechanisch) von außen oder durch aktives Öffnen von innen möglich sein.	Mindestanforderung
Sicherung	Zutrittsmittel (elektronische Zugangssicherungen wie Firmenausweis oder Token und mechanische Schlüssel) MÜSSEN immer gesichert aufbewahrt werden.	Nicht vergebene Zutrittsmittel SOLLEN in einem Safe oder einem abgesicherten Schrank aufbewahrt werden.
Autorisierung	Zutritt durch Mitarbeiter DARF erfolgen.	Absicherung erfolgt durch elektronische Zugangssicherung mit Firmenausweis, Code oder Token, oder mit mechanischem Schlüssel.
Autorisierung	Zutritt für Externe DARF NUR nach vorheriger Ankündigung oder Anmeldung erfolgen.	Regelung der Zuständigkeit für den Besucherempfang (durch Rezeption, Sekretariat, Mitarbeiter) ist standortspezifisch.
Überwachung	Absicherung außerhalb der normalen Arbeitszeiten SOLL durch Alarmanlage mit angeschlossenem Sicherheitsdienst erfolgen.	Soweit am Standort vorhanden.
Überwachung	Überwachung SOLL durch Videokameras erfolgen soweit sinnvoll und technisch möglich.	Soweit am Standort vorhanden.
Überwachung	Überwachung durch Bewegungsmelder SOLL erfolgen.	Alarmierung durch Bewegungsmelder in Erdgeschossräumen bei scharfgeschalteter Alarmanlage, soweit am Standort vorhanden.
Begleitung	Externe SOLLEN nach Möglichkeit ständig in Begleitung von KISTERS Mitarbeitern bleiben.	
Begleitung	Bei Post- und Paketdiensten sowie Speditionen MÜSSEN die zuständigen KISTERS Mitarbeiter informiert werden.	Standort-spezifisch zu regeln.
Protokoll	Das Betreten und Verlassen der Bereiche von Externen MUSS protokolliert werden.	Eintragung in Besucherliste an der Rezeption/Sekretariat
Identifikation	Mitarbeiter MÜSSEN ihren Mitarbeiterausweis jederzeit sichtbar tragen.	

Maßnahme	Umsetzung	Bemerkungen
Identifikation	Externe MÜSSEN ihren Besucherausweis jederzeit sichtbar tragen.	
Verhalten	Personen mit unbekannter oder unklarer Zutrittsberechtigung MÜSSEN angesprochen und deren Zutrittsberechtigung MUSS überprüft werden.	Die Überprüfung SOLL am Empfang vor dem Betreten der kontrollierten Innenbereiche erfolgen.
Verhalten	Wenn Externe beim Verlassen des Bereichs Gegenstände mitführen, SOLLEN diese beim Auschecken auf Rechtmäßigkeit der Mitnahme überprüft werden.	Betrifft insb. Dokumente, Material, Rechner, etc. die mit KISTERS-Signaturen oder Logos gekennzeichnet sind.
Verhalten	Foto-, Video-, Audio- und andere Aufzeichnungen durch Mitarbeiter DÜRFEN NUR für dienstliche Zwecke erstellt werden.	Aufzeichnungen SOLLEN nur mit KISTERS-Systemen erstellt werden. Die Aufzeichnungen MÜSSEN entsprechend der Klassifikation der aufgezeichneten Information klassifiziert werden. Datenschutzbestimmungen MÜSSEN beachtet werden.
Verhalten	Foto-, Video-, Audio- und andere Aufzeichnungen durch Externe DÜRFEN NUR mit Genehmigung des besuchten Mitarbeiters bzw. Organisators erstellt werden.	Die Aufzeichnungen MÜSSEN entsprechend der Klassifikation der aufgezeichneten Information klassifiziert werden. Information der Klassifikation „KISTERS intern“ oder höher DARF von Externen NUR nach Unterzeichnung einer Geheimhaltungsvereinbarung aufgezeichnet werden. Datenschutzbestimmungen MÜSSEN beachtet werden.
Verhalten	Informationen auf ggf. vorhandene Flipcharts, Whiteboards oder andere Utensilien in Schulungs-, Besprechungs-, und Demoräume MÜSSEN vor Verlassen des Raumes entfernt/unkenntlich gemacht werden.	Soweit am Standort vorhanden. Die Entfernung muss nicht erfolgen, wenn die Informationen für direkt anschließende Termine in diesem Raum noch benötigt werden.

Folgende Information MUSS in die Besucherliste eingetragen werden:

(1) Name des/der Externen
(2) Ggfs. Firma/Organisation
(3) Zweck des Besuchs
(4) Uhrzeit Zutritt
(5) Uhrzeit Verlassen
(6) Name der besuchten Person (KISTERS Mitarbeiter) bzw. des Organisators (bei Veranstaltungen)

3.3.3 Interne Bereiche (Z2)

Zusätzlich zu den Maßnahmen für Kontrollierte Innenbereiche gelten die folgenden Maßnahmen:

Maßnahme	Umsetzung	Bemerkungen
Sicherung	Zutritt DARF NUR unter Verwendung des Firmenausweises bzw. eines Firmenschlüssels möglich sein.	Mindestanforderung
Vereinbarung	Externe MÜSSEN eine Geheimhaltungsvereinbarung (Non Disclosure Agreement, NDA) unterzeichnen, wenn sie nicht angekündigt sind und den besuchten Mitarbeitern nicht persönlich bekannt sind.	
Begleitung	Externe MÜSSEN jederzeit in Begleitung eines KISTERS Mitarbeiters bleiben.	Externe MÜSSEN im Eingangsbereich vom besuchten Mitarbeiter abgeholt werden.
Begleitung	Für Externe, die sich regelmäßig in KISTERS Betriebsstätten aufhalten (z.B. Handwerker), KÖNNEN von den Leitern der Standorte Sondergenehmigungen erteilt werden, die diesen Externen den unbegleiteten Aufenthalt in den Betriebsstätten erlauben.	Die Begleitung KANN bei Erteilung einer Zutrittserlaubnis vom Leiter des Standorts entfallen; Zutrittserlaubnis erfordert Geheimhaltungsvereinbarung.
Verhalten	Die Räume (Fenster, Türen) SOLLEN beim (zeitweiligen) Verlassen verschlossen werden.	Die Räume MÜSSEN zwingend verschlossen werden, wenn keine anderweitige Zutrittssicherung existiert.
Verhalten	Beim Verlassen der Räume MÜSSEN diese auf anwesende Personen kontrolliert werden. Mitarbeiter, die die Räume als letzte verlassen, MÜSSEN diese verschließen/abschließen.	Derjenige, der als letzter Räume oder Gebäude verlässt, ist für deren Absicherung verantwortlich; individuelle standort-spezifische Regelungen sind möglich.
Verhalten	Die Alarmanlage MUSS beim Verlassen der Räume am späten Nachmittag scharfgeschaltet werden.	Derjenige, der als letzter Räume oder Gebäude verlässt, ist für die Einschaltung der Alarmanlage verantwortlich; individuelle standort-spezifische Regelungen sind möglich.
Verhalten	Mitarbeiter MÜSSEN unbekannte Personen ohne sichtbaren Ausweis und Externe ohne Begleitung durch Mitarbeiter ansprechen und identifizieren. Diese Personen MÜSSEN für die Registrierung zum Empfang begleitet werden.	
Verhalten	Bei aggressivem oder offensichtlich widerrechtlichem Verhalten (Diebstahl, Sabotage o.ä.) MUSS unverzüglich die Standortleitung und ggfs. die Polizei alarmiert werden.	Kein persönliches Risiko eingehen, Alarmierung ist wichtiger!
Revision	Die vergebenen Zutrittsrechte und Zutrittsmittel MÜSSEN anlassbezogen, mindestens aber einmal jährlich stichprobenartig überprüft werden.	Erfolgt durch den Systemverantwortlichen
Revision	Nicht mehr benötigte Zutrittsrechte und Zutrittsmittel MÜSSEN anlassbezogen bzw. nach Prüfung umgehend entzogen werden.	

3.3.4 Sicherheitsbereiche (Z3)

Zusätzlich zu den Maßnahmen für Interne Bereiche gelten die folgenden Maßnahmen:

Maßnahme	Umsetzung	Bemerkungen
Sicherung	Zutritt DARF NUR unter Verwendung eines Firmenausweises mit spezieller Freigabe bzw. eines separaten Schlüssels möglich sein.	Mindestanforderung
Autorisierung	Autorisierung MUSS durch den KISTERS Vorstand bzw. berechtigte Vertreter am Standort erfolgen.	Regelung durch Übergabe von Schlüssel oder Token oder Freischaltung des Firmenausweises
Autorisierung	Mitarbeiter MÜSSEN für den Zutritt autorisiert sein.	Absicherung erfolgt durch Firmenausweis, Code oder Token, oder mechanischem Schlüssel
Vereinbarung	Externe MÜSSEN eine Geheimhaltungsvereinbarung (Non Disclosure Agreement, NDA) unterzeichnen.	Die Geheimhaltungsvereinbarung KANN firmen- oder personenbezogen sein.
Begleitung	Externe MÜSSEN in permanenter Begleitung eines autorisierten KISTERS Mitarbeiters bleiben.	Die Begleitung KANN beim Vorliegen einer Zutrittserlaubnis vom KISTERS Vorstand oder eines berechtigten Vertreters entfallen; Zutrittserlaubnis erfordert Geheimhaltungsvereinbarung.
Verhalten	Die Räume (Fenster, Türen) MÜSSEN bei jedem Verlassen abgeschlossen werden.	Die Räume MÜSSEN jederzeit abgeschlossen sein, wenn sich kein Mitarbeiter darin aufhält.
Revision	Die vergebenen Zutrittsrechte MÜSSEN anlassbezogen, mindestens aber einmal halbjährlich stichprobenartig überprüft werden.	Erfolgt durch den Systemverantwortlichen
Revision	Zutrittsrechte, die über einen Zeitraum von 6 Monaten nicht genutzt wurden, MÜSSEN gesperrt werden.	Ausnahmen KÖNNEN vom KISTERS Vorstand oder einem berechtigten Vertreter gewährt werden.

3.3.5 Hochsicherheitsbereiche (Z4)

Zusätzlich zu den Maßnahmen für Sicherheitsbereiche gelten die folgenden Maßnahmen:

Maßnahme	Umsetzung	Bemerkungen
Sicherung	Zutritt MUSS über die Vereinzelungsschleuse erfolgen.	Mindestanforderung Für Einzelpersonen im Normalbetrieb
Sicherung	Die Vereinzelungsschleuse DARF NUR kurzzeitig in Ausnahmefällen außer Kraft gesetzt werden.	Materialtransport, Besichtigung/Begutachtung durch nicht speziell autorisierte Personen
Autorisierung	Spezielle Autorisierung MUSS durch den Leiter IT oder den Vorstand erfolgen.	Autorisierung erfolgt durch spezielle Konfiguration des Firmenausweises oder persönliche Registrierung am Zugangssystem
Autorisierung	Mitarbeiter MÜSSEN für den Zutritt spezielle Autorisierung besitzen.	z.B. IT-Administratoren; Absicherung erfolgt durch spezielle Konfiguration des Firmenausweises
Überwachung	Verstärkte Überwachung MUSS durch Videokameras erfolgen.	Zusätzliche Videokameras am Eingangsbereich

Maßnahme	Umsetzung	Bemerkungen
Begleitung	Externe MÜSSEN in permanenter Begleitung eines speziell autorisierten KISTERS Mitarbeiters bleiben.	Die Begleitung KANN beim Vorliegen einer Zutrittserlaubnis vom KISTERS Vorstand oder eines berechtigten Vertreters entfallen.
Protokoll	Jeder Zutritt MUSS protokolliert werden a) Automatische Protokollierung des Zutritts für autorisiertes Mitarbeiter b) Manuelle Protokollierung des Zutritts von Externen durch den begleitenden KISTERS Mitarbeiter	a) Erfolgt durch Sicherungsanlage b) Eintragung in separate Besucherliste für Hochsicherheitsbereiche
Revision	Die vergebenen Zutrittsrechte und Zutrittsmittel MÜSSEN mindestens einmal vierteljährlich stichprobenartig überprüft werden.	Erfolgt durch den Leiter IT
Revision	Zutrittsrechte und Zutrittsmittel, die über einen Zeitraum von 2 Monaten nicht genutzt wurden, MÜSSEN gesperrt werden.	Ausnahmen KÖNNEN vom KISTERS Vorstand oder einem berechtigten Vertreter gewährt werden.
Revision	Zutrittsrechte und Zutrittsmittel, die über einen Zeitraum von 6 Monaten nicht genutzt wurden, MÜSSEN vollständig entzogen werden.	Ausnahmen KÖNNEN vom KISTERS Vorstand oder einem berechtigten Vertreter gewährt werden.

4 Zugangskontrolle

[INFO] Alle IT-Systeme und Anwendungen der KISTERS Gruppe werden durch die Maßnahmen der Zugangskontrolle vor unberechtigter Nutzung und Missbrauch geschützt.
Für jedes IT-System bzw. jede Anwendung MÜSSEN adäquate Maßnahmen für die Kontrolle und Überwachung des logischen Zugangs festgelegt werden.
Die Freigabe zur Nutzung MUSS durch die Einrichtung von Nutzerkonten und die Bekanntgabe der Authentifikationsinformation (Kontenname, Passwort, ggfs. weitere Authentifikationsmechanismen) durch die Systemverantwortlichen erteilt werden. Die Verwendung von Passwörtern regelt die „KISTERS Passwortrichtlinie“.
Vor der Freigabe eines Zugangs MÜSSEN die Berechtigungen des Nutzers innerhalb des IT-Systems bzw. der Applikation hinsichtlich der Nutzung von Funktionen und des Zugriffs auf Daten festgelegt werden (Zugriffskontrolle, Autorisierung).

4.1 Systemklassifikation

Für die Zugangsregelung von IT-Systemen und Anwendungen der KISTERS Gruppe gilt folgende Systemklassifikation nach Nutzerprofilen:

	Systemklasse	Beschreibung / Beispiele
S0	Öffentlich	• Öffentlich zugängliche Webseiten und Applikationen • Webseiten und Applikationen mit Selbstregistrierung • KISTERS Webportale (www.kisters.de, www.kisters.eu, …)
S1	Kontrolliert	• Öffentlich zugängliche Webseiten und –Applikationen mit Registrierung und zusätzlicher Autorisierung/Freischaltung durch KISTERS • KISTERS Service Portal, Jira, Foren • KISTERScloud: Demo-Systeme und –Applikationen

	Systemklasse	Beschreibung / Beispiele
		• ftp-Server, gemeinsam genutzte Office365-Dienste (SharePoint, OneDrive)
S2	Intern	• Alle IT-Systeme und Anwendungen, die ausschließlich von KISTERS genutzt werden • Arbeitsplatzrechner, allgemeine Server • Interne Informationssysteme und Anwendungen (HAL Notes Applications, SITE, Confluence, Jira (interne Projekte), …)
S3	Dediziert	• Alle IT-Systeme und Anwendungen mit eingeschränktem internen oder externen Nutzerkreis • Dedizierte Server (Build-Server, Testserver, …) • Dedizierte Informationssysteme (Sage KHK, NCC, …) • Fernwartungssysteme mit Zugang zu Kundensystemen • Nicht-öffentlich zugängliche, kundenspezifische Systeme (KISTERS-cloud-Systeme, kundenspezifische Testsysteme) • Von externen Dritten zur Verfügung gestellte IT-Systeme für spezielle Zwecke (Entwicklung, Fernwartung, …)
S4	Administrativ	• Infrastruktur (Router, Firewalls, Notes-Server, Microsoft Active Directory, Backup System, Rechenzentrumsinfrastruktur, …) • Managementsysteme für IT-Infrastruktur

Die Zuordnung von IT-Systemen und Anwendung zu den Systemklassen ergibt sich automatisch aus dem Zweck und den vorgesehenen Benutzergruppen.

4.2 Zugangsberechtigungen

Die Zugangsberechtigungen der Personengruppen zu den IT-Systemen und Anwendungen sind in der folgenden Tabelle zusammengefasst:

\Gruppe System	**G0 (jeder)**	**G1 (Externe)**	**G2 (KISTERS)**	**G3 (Autorisierte)**	**G4 (Spez. Aut.)**
S0 (öffentlich)	X	X	X	X	X
S1 (kontrolliert)	-	1	X	X	X
S2 (intern)	-	2,5	X	X	X
S3 (dediziert)	-	2,4,5	2,3,4	2,3,4	2,3,4
S4 (administrativ)	-	2	2	2	2,3

-: kein Zugang

X: uneingeschränkter Zugang

1: Zugang nur nach Freigabe durch einen KISTERS Mitarbeiter

2: Zugang nur mit Überwachung durch einen KISTERS Mitarbeiter mit Freigabe für das System

3: Zugang nur für KISTERS Mitarbeiter mit Freigabe für das System

4: Zugang nur nach Freigabe durch einen autorisierten Vertreter des Kunden

5: Zugang ohne Überwachung nur mit Freigabe durch den KISTERS Vorstand, den Leiter IT oder einen autorisierten Vertreter

4.3 Maßnahmen zur Zugangskontrolle und Überwachung

Für die oben beschriebenen Systemklassen gelten die im Folgenden aufgeführten Kontroll- und Überwachungsmaßnahmen für den logischen Zugang.

4.3.1 Öffentliche Systeme (S0)

Maßnahme	Umsetzung	Bemerkungen
Überwachung	Auffällige Systemaktivitäten SOLLEN der IT-Administration oder dem Systemverantwortlichen durch automatische Alarmierung gemeldet werden.	Systemspezifisch nach Stand der Technik
Überwachung	Das System SOLL durch das „Intrusion Detection System“ des Security Operation Centers überwacht werden.	Systemspezifisch nach Stand der Technik
Protokoll	Überwachung SOLL durch Protokollierung der Nutzung (An- und Abmeldungen) erfolgen.	Systemspezifisch nach Stand der Technik

4.3.2 Kontrollierte Systeme (S1)

Maßnahme	Umsetzung	Bemerkungen
Autorisierung	Zugang zum System durch Mitarbeiter DARF erfolgen.	
Autorisierung	Zugang für Externe DARF NUR nach vorheriger Registrierung und Freigabe erfolgen.	Freigabe erfolgt durch Systemverantwortlichen
Autorisierung	Soweit technisch möglich SOLLEN Zugänge personalisiert sein.	Die Nutzung von gemeinsam genutzten Zugängen MUSS vom Systemverantwortlichen genehmigt werden.
Sicherung	Zur Anmeldung MUSS mindestens eine Benutzerkennung und ein Passwort notwendig sein.	
Sicherung	Sprach-aktivierte Applikationen MÜSSEN deaktiviert sein.	Z.B. Cortana, Siri, Alexa, etc.
Sicherung	Der Zugang MUSS beim Verlassen gesperrt werden, auch bei kurzzeitiger Abwesenheit.	Sperrung KANN durch passwort-geschützten Sperrbildschirm bzw. „Suspendierung“ einer Sitzung mit passwort-geschützter Reaktivierung erfolgen.
Überwachung	Auffällige Systemaktivitäten SOLLEN der IT-Administration oder dem Systemverantwortlichen durch automatische Alarmierung gemeldet werden.	Systemspezifisch nach Stand der Technik
Überwachung	Das System SOLL durch das „Intrusion Detection System“ (IDS) des Security Operation Centers überwacht werden. Systeme, die von KISTERS betrieben werden, MÜSSEN durch das IDS überwacht werden.	Systemspezifisch nach Stand der Technik
Protokoll	Die Nutzung des Systems (An- und Abmeldungen) MUSS protokolliert werden.	Protokollierung über System- und Applikationslogs
Revision	Die vergebenen Zugangsrechte MÜSSEN anlassbezogen, mindestens aber einmal jährlich stichprobenartig überprüft werden.	Erfolgt durch den Systemverantwortlichen

Maßnahme	Umsetzung	Bemerkungen
Revision	Nicht mehr benötigte Zugangsrechte MÜSSEN anlassbezogen bzw. nach Prüfung umgehend entzogen werden.	
Verhalten	Beim Verlassen des Arbeitsplatzes MUSS der Zugang zum System gesperrt werden.	Clear Screen Policy
Verhalten	Bei voraussichtlich längerer Abwesenheit vom Arbeitsplatz SOLL eine Abmeldung vom System erfolgen.	
Verhalten	Es MUSS eine Abmeldung vom System erfolgen, wenn keine Sperrung im aktiven Zustand möglich ist.	
Verhalten	Nicht-autorisierte Zugangsversuche MÜSSEN der IT-Administration und den Systemverantwortlichen gemeldet werden.	

4.3.3 Interne Systeme (S2)

Zusätzlich zu den Maßnahmen für Kontrollierte Systeme gelten die folgenden Maßnahmen:

Maßnahme	Umsetzung	Bemerkungen
Vereinbarung	Externe Nutzer MÜSSEN eine Geheimhaltungsvereinbarung (Non Disclosure Agreement, NDA) unterzeichnen.	
Sicherung	Der Zugang über öffentliche Systeme MUSS verschlüsselt und über Multi-Faktor-Authentifizierung abgesichert sein.	Absicherung über VPN
Sicherung	Jedes IT-System mit interaktivem Benutzerzugang MUSS über einen aktivierten Bildschirmschoner mit Kennwortschutz verfügen.	
Überwachung	Externe Nutzer MÜSSEN bei der Arbeit an dem System von einem autorisierten KISTERS Mitarbeiters überwacht werden.	Die Überwachung KANN beim Vorliegen einer Zutrittserlaubnis vom KISTERS Vorstand oder eines autorisierten Vertreters entfallen; Zugangserlaubnis erfordert Geheimhaltungsvereinbarung.

4.3.4 Dedizierte Systeme (S3)

Zusätzlich zu den Maßnahmen für Interne Systeme gelten die folgenden Maßnahmen:

Maßnahme	Umsetzung	Bemerkungen
Autorisierung	Die Autorisierung für Mitarbeiter SOLL durch die Teamleiter / Vorgesetzten beantragt bzw. freigegeben werden.	Antrag über Ticket
Autorisierung	Mitarbeiter MÜSSEN durch den Systemverantwortlichen autorisiert werden.	Regelung durch Übergabe/Bekanntmachung von Authentifizierungsdaten (Benutzerkennung, Passwort)
Autorisierung	Die Freigabe für Externe MUSS durch den einen autorisierten Vertreter des Kunden/Partners erfolgen.	Regelung durch Übergabe/Bekanntmachung von Authentifizierungsdaten (Benutzerkennung, Passwort)

Maßnahme	Umsetzung	Bemerkungen
Sicherung	Zur Anmeldung KANN eine Multi-Faktor-Authentisierung gefordert werden.	
Sicherung	Administrative Zugänge für Externe MÜSSEN über Multi-Faktor-Authentifizierung abgesichert sein.	
Revision	Die vergebenen Zugangsrechte MÜSSEN anlassbezogen, mindestens aber einmal halbjährlich stichprobenartig überprüft werden.	Erfolgt durch den Systemverantwortlichen
Revision	Zugangsrechte, die über einen Zeitraum von 6 Monaten nicht genutzt wurden, MÜSSEN gesperrt werden.	Ausnahmen KÖNNEN vom KISTERS Vorstand oder einem berechtigten Vertreter gewährt werden.

4.3.5 Administrative Systeme (S4)

Zusätzlich zu den Maßnahmen für Dedizierte Systeme gelten die folgenden Maßnahmen:

Maßnahme	Umsetzung	Bemerkungen
Autorisierung	Die spezielle Freigabe MUSS durch den Leiter IT oder den Vorstand erfolgen.	Regelung durch Übergabe/Bekanntmachung von Authentifizierungsdaten (Benutzerkennung, Passwort)
Autorisierung	Mitarbeiter MÜSSEN für den Zugang eine spezielle Freigabe besitzen (z.B. IT-Administratoren).	Absicherung durch Benutzerkennung und Passwort, ggfs. durch weitere Authentifizierungsmechanismen (Multi-Faktor-Authentifizierung)
Revision	Die vergebenen Zutrittsrechte MÜSSEN anlassbezogen, mindestens aber einmal vierteljährlich stichprobenartig überprüft werden.	Erfolgt durch den Systemverantwortlichen
Revision	Zugangsrechte, die über einen Zeitraum von 2 Monaten nicht genutzt wurden, MÜSSEN gesperrt werden.	Ausnahmen KÖNNEN vom KISTERS Vorstand oder einem berechtigten Vertreter gewährt werden.
Revision	Zugangsrechte, die über einen Zeitraum von 6 Monaten nicht genutzt wurden, MÜSSEN vollständig entzogen werden.	Ausnahmen KÖNNEN vom KISTERS Vorstand oder einem berechtigten Vertreter gewährt werden.

5 Zugriffskontrolle

[INFO] Alle Informationen, Daten und Dokumente der KISTERS Gruppe werden durch die Maßnahmen der Zugriffskontrolle vor unberechtigter Nutzung, Abfluss, Missbrauch und Manipulation geschützt.
Für alle Informationen, Daten und Dokumente MÜSSEN adäquate Maßnahmen zur Kontrolle und Überwachung des Zugriffs festgelegt werden.

5.1 Klassifikation von Information

Für die Zugriffsregelung auf Informationen, Daten und Dokumente der KISTERS Gruppe gilt folgende Klassifikation:

	Klassifikation	Beschreibung / Beispiele
I0	Öffentlich	• Öffentlich zugängliche Webseiten und Publikationen • Firmen-, Produktbroschüren

	Klassifikation	Beschreibung / Beispiele
		• öffentliche Präsentationen
I1	Kontrolliert	• Information in registrierungspflichtigen, nicht kundenspezifischen Kundenbereichen im KISTERS Serviceportal und in Foren • Produktbezogene Handbücher, Manuals, Release Notes, Sicherheitsmeldungen, Arbeitsanleitungen, etc. • Präsentationen für allgemeine Kundenveranstaltungen
I2	Intern	**Standard/Default** für alle Informationen, Daten und Dokumente der KISTERS Gruppe, die nicht anderweitig gekennzeichnet sind oder einem zusätzlichen Zugriffsschutz unterliegen • Information im KISTERS Intranet (HAL Notes DBs, SITE, D3, Confluence, Jira, …) • Allgemeine interne E-Mail • Firmen- und Geschäftsinformation aus internen Veranstaltungen • Interne Entwicklungsinformationen, Spezifikationen • Beschreibungen von Gebäuden und IT-Systemen • Richtlinien, Arbeitsanweisungen, Prozessbeschreibungen, Organigramme • Protokolle, Präsentationen, Projektinformation • Preislisten • Dienstliche Kontaktdaten von Mitarbeitern, Kunden, Partnern und Zulieferern

I3	Vertraulich	• Information mit eingeschränkter Zugriffsberechtigung
		• Kritische Entwicklungspläne, Spezifikationen, Source-Code der KISTERS Lösungen
		• Wettbewerb, Finanzen, Rechtslage, Vertriebspläne
		• Angebotskalkulation und -bewertung, Bid-Management
		• Alle personenbezogenen Daten mit Ausnahme von dienstlichen Kontaktdaten:
		  ○ Mitarbeiterdaten: Bewerbungen, Verträge, Aufzeichnungen zu Mitarbeitergesprächen, Gehaltsinformation
		  ○ persönliche Daten von Mitarbeitern, Kunden, Partnern und Zulieferern
		• Nicht-öffentlich zugängliche Information von oder über Kunden oder Partner (E-Mails, klassifizierte Information, Geschäftsgeheimnisse, Verträge)
		• Information zu Ausschreibungen, Kunden- oder Partnerprojekten
		• Angebote, Aufträge, Rechnungen etc.
		• Daten für den Zugang zu Kundensystemen (KISTERScloud, Fernwartung)
		• Kundendaten in Kunden- oder KISTERScloud-Systemen
		• Support Tickets von Kunden

I4	Streng Vertraulich	• Information mit stark eingeschränkter Zugriffsberechtigung
		• Besondere Kategorien personenbezogener Daten
		  ○ Politische Meinung, Religion, Weltanschauung
		  ○ Genetische, biometrische, Gesundheitsdaten
		  ○ Sexuelle Orientierung
		• Unternehmensstrategie, strategische Entwicklungsdaten
		• Informationen zu Firmenzusammenschlüssen, Akquisitionen etc.
		• Unterlagen zum Sabotage- und Geheimschutz

5.2 Zugriffsberechtigungen

Die Zugriffsberechtigungen der Personengruppen zu den Daten und Informationen sind in der folgenden Tabelle zusammengefasst:

\Gruppe Klassifikation\	G0 (jeder)	G1 (Externe)	G2 (KISTERS)	G3 (Autorisierte)	G4 (Spez. Aut.)
I0 (öffentlich)	X	X	X	X	X
I1 (kontrolliert)	-	X	X	X	X
I2 (intern)	-	1	X	X	X
I3 (vertraulich)	-	1,3	2	2,3	2,3
I4 (streng vertraulich)	-	4	4	4	2,4

-: kein Zugang
X: uneingeschränkter Zugriff
1: Zugriff nur nach Freigabe durch einen autorisierten KISTERS Mitarbeiter
2: Zugriff für KISTERS Mitarbeiter mit Freigabe für die Information
3: Zugriff nach Freigabe durch einen autorisierten Vertreter des Kunden
4: Zugriff nur mit Freigabe durch den KISTERS Vorstand

5.3 Maßnahmen zur Zugriffskontrolle und Überwachung

Unabhängig von der oben beschriebenen Klassifikation von Information gelten folgende Maßnahmen:

- Die Information DARF NUR zu betrieblichen Zwecken genutzt werden.
- Die Freigabe zur Nutzung und Weitergabe von Information MUSS durch Klassifizierung durch den Urheber oder Verantwortlichen für die Information erfolgen.
- Die Klassifikation MUSS durch entsprechende Kennzeichnung der Information kenntlich gemacht werden, sofern dies technisch möglich ist.
- Ein nicht-autorisierter Zugriff auf Informationen, Daten und Dokumente MUSS durch entsprechende technische, personelle und organisatorische Maßnahmen verhindert werden.
- Die Information DARF NUR an berechtigte Empfänger (intern/extern) weitergegeben werden.
- Information, die in IT-Systemen gespeichert ist, MUSS durch die Zugangskontrolle zu den IT-Systemen sowie durch die Autorisierung/Rechtevergabe im IT-System geschützt werden.

Im Einzelnen gelten für die oben beschriebenen Informationsklassen die im Folgenden aufgeführten Kontroll- und Überwachungsmaßnahmen für den Zugriff.

5.3.1 Öffentlich (I0)

Maßnahme	Umsetzung	Bemerkungen
Kennzeichnung	KISTERS Logo oder KISTERS Namenszug SOLL auf allen Seiten der Dokumente oder Webseiten sichtbar sein.	Bei kreativen Werken KANN ein Copyright-Symbol (©) verwendet werden, dies hat jedoch keine weitere rechtliche Relevanz.

5.3.2 Kontrolliert (I1)

Maßnahme	Umsetzung	Bemerkungen
Autorisierung	Information DARF an KISTERS Mitarbeiter weitergegeben werden.	
Autorisierung	Information DARF NUR an registrierte Externe Dritte weitergegeben werden.	Registrierung z.B. durch Anmeldung an KISTERS Serviceportal, Registrierung zu KISTERS Veranstaltungen; Weitergabe von Dokumentation im Rahmen von Produktlizenzen.
Kennzeichnung	KISTERS Logo oder KISTERS Namenszug MUSS auf allen Seiten der Dokumente oder Webseiten sichtbar sein.	Bei kreativen Werken KANN ein Copyright-Symbol (©) verwendet werden, dies hat jedoch keine weitere rechtliche Bedeutung.
Speicherung	Information MUSS vor unkontrolliertem Zugriff durch nicht autorisierte Externe geschützt sein.	
Übertragung	Information DARF an registrierte oder namentlich benannte Externe versandt werden.	Post oder elektronische Übertragung ohne Verschlüsselung ist erlaubt.
Vernichtung	Papierdokumente MÜSSEN zerrissen oder geschreddert werden.	
Vernichtung	Elektronische Dokumente auf nicht-firmeneigenen Datenträgern MÜSSEN gelöscht werden	Gilt z.B. bei der Nutzung von externe IT-Systeme für Präsentationen
Revision	Die Informationsklassifikation MUSS anlassbezogen, mindestens aber einmal jährlich stichprobenartig überprüft werden.	Erfolgt durch den Verantwortlichen für die Information

5.3.3 Intern (I2)

Zusätzlich zu den Maßnahmen für Kontrollierte Information gelten die folgenden Maßnahmen:

Maßnahme	Umsetzung	Bemerkungen
Autorisierung	Information DARF an KISTERS Mitarbeiter weitergegeben werden.	
Vereinbarung	Externe MÜSSEN eine Geheimhaltungsvereinbarung unterzeichnen, bevor sie Zugriff auf die Information erhalten.	
Kennzeichnung	Information SOLL als „**intern**“ oder „**internal**“ gekennzeichnet sein.	**Nicht gesondert gekennzeichnete Informationen in elektronischer oder Papierform sind immer als Intern klassifiziert.**
Speicherung	Information DARF NICHT auf privaten Datenträgern gespeichert werden.	
Speicherung	Externe Cloud-Speicher MÜSSEN für die Speicherung von Information vom CISO genehmigt werden.	Gilt u.a. für Dropbox, OneDrive (allgemein), Google Drive, etc. Ausnahmen: Gilt nicht für Microsoft OneDrive der Domäne kag2021 und den Atlassian Cloud Mandanten conflks.
Speicherung	Information MUSS vor der Speicherung in externen Cloud-Speichern verschlüsselt werden.	Ausnahmen: Gilt nicht für Microsoft OneDrive der Domäne kag2021 und

Maßnahme	Umsetzung	Bemerkungen
		den Atlassian Cloud Mandanten conflks.
Transport / Übertragung	Information SOLL bei elektronischer Übertragung an Externe verschlüsselt werden.	
Transport / Übertragung	Ausdrucke elektronischer Dokumente MÜSSEN unmittelbar nach Absenden des Druckauftrags vom Drucker abgeholt werden.	

5.3.4 Vertraulich (I3)

Zusätzlich zu den Maßnahmen für Interne Information gelten die folgenden Maßnahmen:

Maßnahme	Umsetzung	Bemerkungen
Autorisierung	Freigabe für Mitarbeiter und primäre externe Informationsempfänger MUSS durch den Urheber bzw. Verantwortlichen für die Information erfolgen.	Regelung durch Übergabe/Bekanntmachung von Authentifizierungsdaten (Kontenname, Passwort) oder Gruppenzuordnung; Verteilerliste bei Papierdokumenten.
Autorisierung	Freigabe für Externe MUSS durch den einen autorisierten Vertreter des Kunden/Partners erfolgen.	Regelung durch Übergabe/Bekanntmachung von Authentifizierungsdaten (Kontenname, Passwort); Verteilerliste bei Papierdokumenten.
Sicherung	Information DARF NUR an autorisierte KISTERS Mitarbeiter und autorisierte Externe weitergegeben werden (minimum-need-to-know-principle).	
Sicherung	Mitarbeiter und Externe MÜSSEN für den Zugriff auf elektronische Information autorisiert sein.	Absicherung durch Benutzerkennung und Passwort oder Gruppenzuordnung.
Kennzeichnung	Information MUSS als „**vertraulich**“ oder „**confidential**“ gekennzeichnet sein.	Vertraulichkeitskennzeichnung SOLL auf jeder Seite des Dokuments sichtbar sein.
Kennzeichnung	Information SOLL mit Zweck der Information oder Informationsempfänger gekennzeichnet sein.	Zweck oder Empfänger SOLL auf jeder Seite des Dokuments sichtbar sein.
Speicherung	Kopien DÜRFEN NUR nach Rücksprache mit dem Urheber bzw. Verantwortlichen erstellt werden	
Speicherung	Papierdokumente MÜSSEN in verschlossenen Räumen oder Schränken mit physischem Zugriffsschutz gelagert werden.	
Speicherung	Elektronische Information MUSS auf mobilen Datenträgern verschlüsselt werden.	
Speicherung	Elektronische Information DARF NICHT auf privaten Datenträgern gespeichert werden.	
Transport / Übertragung	Papierdokumente MÜSSEN physisch vor unberechtigtem Zugriff geschützt werden.	
Transport / Übertragung	Papierdokumente MÜSSEN intern und extern in einem verschlossenen Umschlag mit Vermerk "Persönlich / Vertraulich" weitergegeben werden.	

Maßnahme	Umsetzung	Bemerkungen
Transport / Übertragung	Elektronische Dokumente DÜRFEN NUR auf Druckern mit physischem Zugangsbeschränkung für autorisierte Personen oder bei Anwesenheit von autorisierten Personen am Drucker ausgedruckt werden.	Falls dies nicht möglich ist (z.B. an kleinen Standorten mit Gemeinschaftsdrucker) MUSS der Drucker mindestens in einem internen Bereich stehen und der Zeitpunkt des Druckens MUSS so gewählt werden, dass ein unbefugter Zugriff weitestgehend ausgeschlossen ist.
Transport / Übertragung	Interne E-Mails MÜSSEN in Outlook mit Vertraulichkeit „**Privat**“ gekennzeichnet werden.	Die Kennzeichnung "Privat" in Outlook verweigert den Stellvertretern, die Zugriff auf das E-Mail-Konto des Empfängers haben, den Zugriff auf die E-Mail. Achtung: weder die Kennzeichnung "Persönlich" noch "Vertraulich" haben diesen Effekt!
Transport / Übertragung	Elektronische Dokumente MÜSSEN an Externe über zugriffs- und transportgesicherte Medien übertragen werden.	Default-Mechanismen SOLLEN die Übertragung über sftp über den KISTERS ftp-server mit dedizierten Nutzerkonten oder die Nutzung von S/MIME-verschlüsselte E-Mail sein. Andere Übertragungsmechanismen KÖNNEN mit den Externen individuell vereinbart werden.
Transport / Übertragung	Passwörter MÜSSEN immer verschlüsselt übertragen werden.	Verschlüsselte E-Mail oder „KISTERS privatebin“.
Vernichtung	Papierdokumente MÜSSEN mit Aktenvernichter der Klasse 4 geschreddert werden.	
Revision	Die vergebenen Zugriffsrechte MÜSSEN anlassbezogen, mindestens aber einmal halbjährlich stichprobenartig überprüft werden.	Erfolgt durch den Verantwortlichen für die Information.

5.3.5 Streng Vertraulich (I4)

Zusätzlich zu den Maßnahmen für Vertrauliche Information gelten die folgenden Maßnahmen:

Maßnahme	Umsetzung	Bemerkungen
Autorisierung	Spezielle Freigabe MUSS durch den KISTERS Vorstand oder einen autorisierten Vertreter erfolgen.	Regelung durch Übergabe/Bekanntmachung von Authentifizierungsdaten (Kontenname, Passwort) oder Gruppenzuordnung; Verteilerliste bei Papierdokumenten.
Autorisierung	Information DARF NUR an namentlich benannte, autorisierte KISTERS Mitarbeiter weitergegeben werden.	Absicherung durch Benutzerkennung und Passwort, ggfs. durch weitere Authentifizierungsmechanismen
Autorisierung	Information DARF NUR an namentlich benannte, autorisierte Externe weitergegeben werden.	Absicherung durch Benutzerkennung und Passwort, ggfs. durch weitere Authentifizierungsmechanismen
Kennzeichnung	Information MUSS als „**streng vertraulich**“ oder „**strictly confidential**“ gekennzeichnet sein.	Vertraulichkeitskennzeichnung MUSS auf jeder Seite des Dokuments sichtbar sein.
Protokoll	Der Empfang der Information MUSS bestätigt werden.	Per Unterschrift oder elektronischer Empfangsbestätigung;

Maßnahme	Umsetzung	Bemerkungen
		Postversand MUSS als Einschreiben erfolgen.
Speicherung	Kopien DÜRFEN NUR nach Genehmigung durch den KISTERS Vorstand erstellt werden.	
Speicherung	Papierdokumente MÜSSEN unter Verschluss gehalten werden.	Lagerung in einem Tresor oder speziell abgesicherten Räumen.
Speicherung	Elektronische Dokumente MÜSSEN verschlüsselt gespeichert werden.	
Transport / Übertragung	Papierdokumente MÜSSEN intern und extern in einem verschlossenen Umschlag mit Vermerk "Persönlich / Streng Vertraulich" weitergegeben werden.	
Transport / Übertragung	Information DARF NUR in Ausnahmefällen außerhalb gesicherter KISTERS Betriebsstätten mitgenommen werden.	
Vernichtung	Die Vernichtung der Information SOLL unter Aufsicht erfolgen (Vier-Augen-Prinzip)	
Revision	Die vergebenen Zugriffsrechte MÜSSEN anlassbezogen, mindestens aber einmal vierteljährlich stichprobenartig überprüft werden.	Erfolgt durch den Verantwortlichen für die Information

6 Klassifikationskriterien

[INFO] Die Klassifikation der Informationswerte erfolgt anhand des Schutzbedarfs gemäß den Schutzzielen Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit. Dabei ist der potentielle Schaden im Fall von Missbrauch, Sabotage, Informationsabfluss oder -manipulation infolge unerlaubten Zutritts, Zugangs oder Zugriffs maßgebend.

6.1 Klassifikation nach Schutzbedarf

Eine angemessene Einstufung von Gebäuden, Systemen und Informationen in die entsprechenden Klassen SOLL anhand folgender Tabelle erfolgen:

Schadenshöhe	Schaden für KISTERS	Klassen
Kein	Kein Schaden, da öffentliche Nutzung vorgesehen	Z0, S0, I0
Sehr niedrig	Keine weitreichenden Konsequenzen, da kontrollierte Nutzung durch Externe vorgesehen	Z1, S1, I1
Niedrig	Geringfügige nachteilige rechtliche Folgen gegenüber Externen Kein bzw. nur sehr geringer Verlust personenbezogener Daten Aufgabenerfüllung ist nicht nennenswert beeinträchtigt (z. B. durch Verlust der Verfügbarkeit, Integrität oder Authentizität) Negative Außenwirkung gering Finanzielle Auswirkungen im geringen Umfang	Z2, S2, I2
Mittel	Verstöße gegen Gesetze, Verordnungen oder Verträge mit spürbaren Konsequenzen (Bußgelder, Geldstrafen)	Z3, S3, I3

Schadenshöhe	Schaden für KISTERS	Klassen
	Personenbezogene Daten im größeren Umfang betroffen Aufgabenerfüllung in einem Unternehmensbereich stark beeinträchtigt (z. B. durch Verlust der Verfügbarkeit, Integrität oder Authentizität) Spürbare Schädigung des Firmenrufs bei Kunden/Partnern Erheblicher finanzieller Schaden	
Hoch bis existenzgefährdend	Fundamentaler Verstoß gegen Gesetze (Haftstrafen) Besondere Kategorien personenbezogener Daten betroffen Aufgabenerfüllung des gesamten Unternehmens gravierend beeinträchtigt (z. B. durch Verlust der Verfügbarkeit, Integrität, Authentizität) Sehr schwerer bis irreparabler Schaden für die KISTERS Geschäftszwecke und Ziele Existenzgefährdender finanzieller Schaden für KISTERS	Z4, S4, I4

6.2 Datenvernichtung nach DIN 66399 / ISO 21964-1

Die Vernichtung von Datenträgern MUSS auf Basis der Klassifikation der betroffenen Information nach den Vorgaben der einschlägigen Normen [5], [6], [7] vorgenommen werden.

[INFO] Die Normen definieren Schutzklassen und Sicherheitsstufen, die für die Vernichtung von Daten und Datenträgern relevant sind.
Die Schutzklassen bewerten Information anhand ihres Schutzbedarfs, gemessen durch den möglichen Schaden bei Kompromittierung der Information. Die Schutzklasse der Information ergibt sich direkt aus der KISTERS Klassifikation.
Die Sicherheitsstufen kennzeichnen qualitativ den Aufwand, der für die Reproduktion / Wiederherstellung von Information nach Vernichtung der Datenträger zu leisten wäre.

Sicherheitsstufe	Aufwand für Reproduktion / Wiederherstellung
1	Eine Reproduktion ist ohne besondere Hilfsmittel und Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand möglich
2	Eine Reproduktion ist nur mit Hilfsmitteln und besonderem Aufwand möglich
3	Eine Reproduktion ist nur mit erheblichem Aufwand möglich (Hilfsmittel, Zeit, Personal)
4	Eine Reproduktion ist nur mit außergewöhnlich hohem Aufwand möglich (Hilfsmittel, Zeit, Personal)
5	Eine Reproduktion ist nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen, sowie forensischen Methoden möglich
6	Eine Reproduktion ist nach dem Stand der Technik unmöglich
7	Eine Reproduktion ist nach dem Stand von Wissenschaft und Technik unmöglich

Im Umkehrschluss ergeben sich daraus entsprechende Kriterien und Vorgaben, die bei der Vernichtung von Daten und Datenträgern eingehalten werden müssen.
Die Zuordnung der Klassifikation zu den in den Normen definierten Schutzklassen und Sicherheitsstufen ist in der folgenden Tabelle dargestellt.

		Sicherheitsstufe						
Klassifikation	**Schutz-klasse**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
I0 (öffentlich)	-	(x)	(x)	(x)	(x)	(x)	(x)	(x)
I1 (kontrolliert)	1	X	X	X	(x)	(x)	(x)	(x)
I2 (intern)	1	X	X	X	(x)	(x)	(x)	(x)
I3 (vertraulich)	2	-	-	X	X	X	(x)	(x)
I4 (streng vertraulich)	3	-	-	-	X	X	X	X

-: nicht anwendbar
X: anwendbar
(x): optional anwendbar (höhere Vernichtungsqualität)

Zur Vereinfachung der internen Handhabung MÜSSEN folgende Vorgaben zur Vernichtung von Datenträgern eingehalten werden:

- Alle Papierdokumente, die Information der Klassifikation I1 oder höher enthalten, MÜSSEN lokal in einem Schredder vernichtet oder zentral in einem geschlossenen Behälter gesammelt werden, der einem zertifizierten Entsorger zur Vernichtung übergeben wird.
- Für Papierdokumente der Klassifikation I3 oder höher MUSS bei lokaler Vernichtung ein Schredder der Sicherheitsstufe 3 oder höher eingesetzt werden.
- Alle anderen Datenträger:
    - optische Datenträger (CD, DVD, etc.),
    - magnetische Datenträger (Disketten, ID-Karten, etc.),
    - Festplatten mit magnetischem Datenträger,
    - elektronische Datenträger (Chipkarten (SD-Karten etc.), Speicherbausteine, Halbleiterfestplatten (SSD), USB-Sticks, mobile Kommunikationsmittel, etc.)

  MÜSSEN zur Vernichtung / Entsorgung an die KISTERS Systemadministration bzw. deren lokalen Stellvertreter übergeben werden.

  [INFO] Diese Datenträger werden entweder durch die Systemadministratoren mechanisch zerstört oder gesammelt an einen zertifizierten Entsorger übergeben.

7 Referenzen

[1] "KISTERS Informationssicherheits-Richtlinie", KISTERS ISMS, Confluence
[2] "KISTERS Information Security Organisation", KISTERS ISMS, Confluence
[3] "KISTERS Information Security Laws and Regulations", KISTERS ISMS, Confluence
[4] “KISTERS Personalmanagement”, KISTERS ISMS, Confluence

[5] “ISO/IEC 21964-1:2018-08: Information technology - Destruction of data carriers - Part 1: Principles and definitions”; International Standards Organization, 2018.

[6] „DIN 66399-1: Büro- Und Datentechnik, Vernichten Von Datenträgern. Teil 1: Büro- und Datentechnik, Vernichten von Datenträgern, Teil 1: Grundlagen und Begriffe“; Oktober 2012. Berlin: Deutsches Institut für Normung e.V, 2012.

[7] „Datenschutzgerechte Datenträgervernichtung - nach dem Stand der Technik“; 4. Auflage, Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), 2019, URL: https://www.gdd.de/wp-content/uploads/2023/06/Datenschutzgerechte-Datentraegervernichtung-4.-Aufl.-2019.pdf (2024-05-03)

[8] „TR-03109-6 Smart-Meter-Gateway-Administration”, v. 1.0., 2015-11-26, Bundesamt für Sicherheit in der Informationstechnik (BSI), URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR-03109-6-Smart_Meter_Gateway_Administration.html (2024-05-03).

8 Dokumenthistorie

Dieses Dokument wird mindestens einmal pro Jahr auf Aktualität geprüft und ggfs. angepasst. Die offizielle Version dieses Dokuments wird online verwaltet. Vor der Verwendung von elektronischen Kopien oder gedruckten Versionen sind diese auf Aktualität zu überprüfen.

Version	Datum	Editor	Aktion
5.7	2025-01-07	J. Rade	Ergänzung Vorgabe Flipchart/Whiteboards in Besprechungsräumen + verstärkte Beachtung Schutzziele Verfügbarkeit, Integrität und Authentizität
5.6	2024-05-03	H.-J. Schlebusch	Ergänzungen/Klarstellungen zur Zugriffskontrolle
5.5	2024-01-22	H.-J. Schlebusch	Regelung für standortspezifische Ausnahmen und Sonderfälle, kleine Ergänzungen und Korrekturen
5.4	2023-12-18	H.-J. Schlebusch	Explizite Aufnahme SMGWA-Arbeitsplatz in Sicherheitsbereiche; Sperren des Arbeitsplatzes zu „kontrollierte Systeme“ verschoben; kleine Ergänzungen und Korrekturen.
5.3	2023-10-10	H.-J. Schlebusch	Ergänzung: Basis der Klassifikation
5.2	2023-09-07	J. Plischke H.-J. Schlebusch	Ergänzung Kapitel „Genehmigung“, „Privilegierte Rechte“ Weitere Ergänzungen und Korrekturen entsprechend C5-Anforderungen
5.1	2023-08-28	J. Weber	Tiefgarage (AC) zurückgestuft von Z1 auf Z0
5.0	2023-04-26	H.-J. Schlebusch	Struktur angepasst an C5 SP-01 Dokumentvorlage; Ergänzungen: Ziele, Anwendungsbereich, Rollen, rechtliche Anforderungen, Referenzen
4.1	2022-09-21	J. Weber H.-J. Schlebusch	Ausnahmen für Microsoft und Atlassian Cloud für interne Information. Kleine Ergänzungen und Fehlerkorrekturen
4.0	2021-10-29	H.-J. Schlebusch	Erweiterung des Titels auf „Klassifikation …“; Mindestanforderungen für die Qualität des Zutritts pro Sicherheits-

Version	Datum	Editor	Aktion
			zone; Regelung für Foto-, Video- und Audioaufzeichnungen für Zone Z1 und höher; Konkretisierung „Datenvernichtung“ nach DIN 66399.
3.6	2020-11-10	H.-J. Schlebusch	Anpassungen wegen Umstellung auf Outlook E-Mail
3.5	2020-09-28	H.-J. Schlebusch	Überprüfung Rechtevergabe: Stichprobenverfahren
3.4	2020-08-04	H.-J. Schlebusch	Ergänzung: IT-Systeme Dritter; Ausnahmegenehmigungen durch Standortleitung
3.3	2020-01-29	H.-J. Schlebusch	Ergänzung „Jira“, Überprüfung und Freigabe
3.2	2019-04-04	H.-J. Schlebusch	sprach-aktivierte Applikationen, Cloud-Speicher, Dokumentenausdruck
3.1	2018-08-15	H.-J. Schlebusch	Fehlerkorrektur, redaktionelle Überarbeitung, Anpassung der englischen Version
3.0	2017-11-21	H.-J. Schlebusch	Reduktion der System- und Informationsklassen auf vier Stufen, Ergänzung Klassifikationskriterien
2.3	2017-07-19	H.-J. Schlebusch	Kleinere Änderungen
2.2	2017-07-10	H.-J. Schlebusch	Kundendaten -> I3 (vertraulich), Erweiterung Kap. 2.3
2.1	2016-11-29	H.-J. Schlebusch	Ergänzung „Rechteüberprüfung“
2.0	2016-10-25	H.-J. Schlebusch	Umbenennung, Erweiterung um Zugangs- und Zugriffskontrolle
1.1	2016-10-18	H.-J. Schlebusch	Revision
1.0	2015-11-21	H.-J. Schlebusch	Erstellung