KISTERS

KISTERS Informations-Sicherheitsrichtlinie

v.5.6, 2025-09-22

Verantwortlich:
KISTERS ISMT

Inhaltsverzeichnis

1 Einleitung

Information und deren Verarbeitung spielt eine Schlüsselrolle für die Aufgabenerfüllung der KISTERS Gruppe. Alle Daten und Informationen, auf die Mitarbeiter im Rahmen ihrer Tätigkeit bei der KISTERS Gruppe Zugriff erhalten, sind grundsätzlich als intern oder vertraulich zu behandeln. Daher ist der Schutz dieser Informationen vor unberechtigtem Zugriff, vor unerlaubter Änderung oder Verbreitung sowie nicht tolerierbarer Unverfügbarkeit von existenzieller Bedeutung. Die „KISTERS Informationssicherheitsleitlinie“ beschreibt die Sicherheitsziele bezüglich Information und IT-Systemen sowie strategische Vorgaben und Randbedingung zu deren Erreichung.
Diese Richtlinie hat zum Ziel, den Mitarbeitern der KISTERS Gruppe konkrete Maßnahmen und Vorgaben für die Erreichung der Sicherheitsziele an die Hand zu geben. Hierzu gehören neben allgemeinen Maßnahmen auch Maßnahmen beim Umgang mit IT-Systemen, die für die Erreichung und Erhaltung von Informationssicherheit zu treffen sind.

1.1 Anwendungsbereich

Diese Informationssicherheitsrichtlinie gilt für alle Mitarbeiter, Geschäftsbereiche, Standorte und die gesamte IT-Infrastruktur der KISTERS Gruppe und der darin betriebenen IT-Systeme. Zur KISTERS Gruppe gehört die KISTERS AG sowie alle ihre nationalen und internationalen Tochterunternehmen. Zu den Mitarbeitern gehören alle Angestellten der KISTERS Gruppe, einschließlich Praktikanten und Aushilfen, sowie alle Mitarbeiter von Drittfirmen und Privatpersonen, die bei der KISTERS Gruppe oder für die KISTERS Gruppe tätig sind.
Die in dieser Richtlinie enthaltenen Sicherheitsregelungen haben für die genannten Personenkreise bindenden Charakter. Grob fahrlässige oder vorsätzliche Verstöße gegen die Informationssicherheitsrichtlinien werden disziplinarisch und (straf-)rechtlich im Rahmen der gesetzlichen Möglichkeiten verfolgt und geahndet.

1.2 Terminologie

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden folgende in Großbuchstaben geschriebenen Schlüsselworte gemäß RFC 2119 verwendet:

- „MUSS“ / „DARF NUR“ oder „VERPFLICHTEND“ bedeuten, dass es sich um eine normative Anforderung handelt. Ausnahmen müssen schriftlich vom KISTERS Vorstand oder einem Beauftragten genehmigt und dokumentiert werden.
- „DARF NICHT“ / „DARF KEIN“ oder „VERBOTEN“ bezeichnen den normativen Ausschluss einer Eigenschaft. Ausnahmen müssen schriftlich vom KISTERS Vorstand oder einem Beauftragten genehmigt und dokumentiert werden.
- „SOLL“ oder „EMPFOHLEN“ beschreiben eine dringende Empfehlung. Abweichungen zu diesen Empfehlungen müssen im Einzelfall begründet und von den Vorgesetzten und/oder Fachverantwortlichen genehmigt werden.
- „SOLL NICHT“ / „SOLL KEIN“ oder „NICHT EMPFOHLEN“ kennzeichnen die dringende Empfehlung, eine Eigenschaft oder Verhalten auszuschließen. Abweichungen zu diesen Empfehlungen müssen im Einzelfall begründet und von den Vorgesetzten und/oder Fachverantwortlichen genehmigt werden.

- „KANN“ oder „OPTIONAL“ bedeuten, dass die Eigenschaft oder das Verhalten wirklich optional ist.

Die Abschnitte dieser Informationssicherheitsrichtlinie sind grundsätzlich als normativ anzusehen. Informative Abschnitte werden explizit am Anfang durch das Schlüsselwort [INFO] gekennzeichnet.

1.3 Ansprechpartner

Das Informationssicherheits-Managementteam ist ständiger Ansprechpartner zu allen Themen der Informationssicherheit, des Datenschutzes und der Geschäftskontinuität:

Name	Rolle	Telefon	E-Mail
Bernd Kisters	CIO (Leiter IT)	+49 2408 9385 105 +49 172 7181704	bernd.kisters@kisters.de
Dr. Heinz-Josef Schlebusch	CISO (Chief Information Security Officer) & DSB (Datenschutzbeauftragter)	+49 2408 9385 226 +49 172 7181829	schlebusch@kisters.de
Jens Weber	BCMO (Business Continuity Management Officer)	+49 2408 9385 126 +49 170 3755187	jens.weber@kisters.de
Jasmina Rade	IS Expert	+49 2408 9385 433 +49 171 1042409	jasmina.rade@kisters.de
Mailbox IT-Sicherheit			itsecurity@kisters.de
Mailbox Datenschutz			datenschutz@kisters.de
Mailbox E-Mail-Sicherheit			mailsecurity@kisters.de
Mailbox System-Administration			sysadmin@kisters.de
Jira Service Desk Informationssicherheit	https://conflks.atlassian.net/servicedesk/customer/portal/11		
Jira Service Desk System-Administration	https://conflks.atlassian.net/servicedesk/customer/portal/5		
Jira Service Desk Whistleblowing	https://conflks.atlassian.net/servicedesk/customer/portal/14		

Ansprechpartner zu technischen Fragen ist die KISTERS IT-Administration (nachfolgend „IT-Administration“ bzw. „IT-Administratoren“ genannt).

1.4 Weitere Informationen

Weitergehende Informationen und Richtlinien zum Thema Informationssicherheit und Datenschutz werden im KISTERS Confluence Compliance Center Space (https://conflks.atlassian.net/wiki/spaces/CC/pages/30049401/Information+Security+and+Data+Protection+Informationssicherheit+und+Datenschutz) veröffentlicht.

Informationen über verfügbare Softwaretools werden von der IT-Administration im KISTERS Confluence General Information Space in der Rubrik „Systemadministration -> Tools & Software“ (https://conflks.atlassian.net/wiki/spaces/GEN/pages/44500611/Tools+Software) zur Verfügung gestellt.

2 Informationssicherheit im Geschäftsbetrieb

2.1 Verpflichtung zur Einhaltung

Die Vorgaben zur Informationssicherheit, zum Datenschutz und zur Geschäftsfortführung sind verbindlich und MÜSSEN bei allen betrieblichen Aktivitäten berücksichtigt werden.
Bei internen und externen Projekten MÜSSEN, unabhängig von der Größe und Art der Projekte, Anforderungen an und Auswirkungen auf Informationssicherheit und Datenschutz identifiziert und bewertet werden. Dazu

- SOLLEN die Ziele der Informationssicherheit, des Datenschutzes und des Business Continuity Managements soweit zutreffend in den Projektzielen enthalten sein;
- SOLL eine Risikobewertung der Informationssicherheit, des Datenschutzes und des Business Continuity Managements in einem frühen Stadium des Projektes durchgeführt werden, um notwendige Sicherheitsmaßnahmen zu identifizieren;
- SOLLEN Informationssicherheit, Datenschutz und Business Continuity Management in allen Phasen der Projektdurchführung berücksichtigt werden.

Bei Projekten und betrieblichen Aktivitäten, die erhebliche Auswirkungen auf die Informationssicherheit, den Datenschutz oder der Geschäftsfortführung haben können, MÜSSEN der CISO, DSB und BCMO frühestmöglich informiert und involviert werden, um notwendige Sicherheits-, Datenschutz- oder BCM Maßnahmen zu identifizieren und mögliche Risiken zu vermeiden.

2.2 Abweichungen und Ausnahmen

Abweichungen und Ausnahmen von den Vorgaben zur Informationssicherheit KÖNNEN zeitlich befristet genehmigt werden. Dazu MÜSSEN die durch die Abweichungen entstehenden Risiken vom jeweiligen Risikoeigentümer bewertet und gemäß den Vorgaben zum Risikomanagement behandelt werden. Die genehmigten Abweichungen, deren zeitliche Befristung sowie die Risikobewertung und -behandlung MÜSSEN geeignet dokumentiert werden, zum Beispiel über entsprechende Tickets im KISTERS Ticketsystem.

3 Zulässige Nutzung von Unternehmenswerten

Unternehmenswerte, die KISTERS Mitarbeiter im Rahmen ihrer Tätigkeit bei der KISTERS Gruppe nutzen, sind DÜRFEN NUR für dienstliche Zwecke verwendet werden. Dazu hören unter anderem Gebäude, Räumlichkeiten, Arbeitsplätze, Geräte, Fahrzeuge, IT-Systeme, Kommunikationssysteme, Anwendungen, Dokumente, Informationen in analoger oder digitaler Form.
Davon abweichend KÖNNEN Unternehmenswerte für nicht-dienstliche Zwecke verwendet werden, wenn eine allgemeine Ausnahmeregelung oder eine spezielle Ausnahmevereinbarung vorliegt.

[INFO] Zur Erreichung und Erhaltung der Informationssicherheit muss eine unberechtigte oder missbräuchliche Nutzung von Unternehmenswerten verhindert werden. Dazu werden Maßnahmen zur Kontrolle von Zutritts-, Zugangs- und Zugriffskontrolle ergriffen:

- Zutrittskontrolle betrifft den physischen Zutritt zu Gebäuden, Räumen und IT-Systemen,
- Zugangskontrolle betrifft die Nutzung von IT-Systemen,
- Zugriffskontrolle betrifft den Zugriff auf jegliche Information, Daten und Dokumente.

Der Schutzbedarf von Gebäuden, IT-Systemen und Information ist abhängig von deren Verwendungszweck und Kritikalität. Daher werden diese Unternehmenswerte klassifiziert und in einem mehrstufigen System entsprechende Maßnahmen zur Erreichung der Sicherheitsziele festgelegt.
Die Klassifizierung und entsprechende Maßnahmen sind in der Richtlinie „KISTERS Klassifikation der Informationswerte - Zutritts-, Zugangs- und Zugriffskontrolle“ festgelegt und sind obligatorischer Bestandteil dieser „KISTERS Informationssicherheitsrichtlinie“. Im Folgenden sind die dort beschriebenen Maßnahmen in vereinfachter Form zusammengefasst.

3.1 Zutrittskontrolle

Jede KISTERS Betriebsstätte (Firmengebäude bzw. Gebäudeteile oder Räume bei angemieteten Räumlichkeiten) MUSS jederzeit gegen unberechtigten Zutritt gesichert sein. Außerhalb der für jeden Standort festgelegten Geschäftszeiten MUSS die Betriebsstätte verschlossen sein. Standort-spezifische Regelungen für den Zutritt und die Absicherung der Betriebsstätten MÜSSEN befolgt werden.
Der Zutritt von Externen MUSS durch Einträge in eine Besucherliste am Empfang bzw. dem Sekretariat protokolliert werden. Externe DÜRFEN sich NUR in Begleitung von KISTERS Mitarbeitern in den internen Bereichen von KISTERS Betriebsstätten aufhalten.
Räume mit hohem Schutzbedarf MÜSSEN immer verschlossen sein. Der Zutritt zu diesen Räumen DARF NUR durch autorisiertes Personal oder in Begleitung von autorisiertem Personal erfolgen. Zu den Räumen mit hohem Schutzbedarf gehören unter anderem Serverräume, Technikräume, Archive und Aktenlager.

3.1.1 Nutzung von Aufzeichnungsgeräten

Innerhalb der KISTERS Betriebsstätten DÜRFEN Foto-, Video-, Audio- und andere Aufzeichnungen durch Mitarbeiter NUR für dienstliche Zwecke erstellt werden. Diese Aufzeichnungen SOLLEN nur mit KISTERS Arbeitsmitteln erstellt werden. Aufzeichnungen MÜSSEN von anderen Aufzeichnungsgeräten gelöscht werden, sobald der Zweck der Aufzeichnungen entfällt oder die Aufzeichnungen auf KISTERS-Systeme übertragen wurden.
Foto-, Video-, Audio- und andere Aufzeichnungen durch Externe Dritte DÜRFEN NUR mit Genehmigung des verantwortlichen KISTERS Mitarbeiters erstellt werden.
Die Aufzeichnungen MÜSSEN entsprechend der Klassifikation der aufgezeichneten Information klassifiziert und behandelt werden. Bei allen Aufzeichnungen MÜSSEN die anwendbaren Datenschutzbestimmungen beachtet werden.

3.2 Zugangskontrolle

Für jedes IT-System bzw. jede Anwendung MÜSSEN adäquate Maßnahmen für die Kontrolle und Überwachung des logischen Zugangs zum Schutz vor unberechtigter Nutzung und Missbrauch festgelegt werden.
Für jede Information, jedes IT-System bzw. jede Anwendung MÜSSEN ein oder mehrere Verantwortliche benannt werden, die für die Erteilung der Zugriffsautorisierung und die Vergabe von Nutzungsrechten (Autorisierung) innerhalb des Systems verantwortlich sind.

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.
Beim Ausscheiden und der Änderung der Rolle eines Mitarbeiters MUSS der Vorgesetzte sofort die Verantwortlichen für die vom Mitarbeiter genutzten Informationen und Systeme informieren und eine Prüfung und ggfs. Änderung der Zugriffs- und Nutzungsrechte und zugehöriger Passwörter veranlassen.

3.2.1 Passwörter

[INFO] Passwörter und PINs („Personal Identification Numbers“) sind vertrauliche Informationen, deren Kompromittierung weitreichende Konsequenzen haben kann.
Die Verwendung von Passwörtern und PINs ist in der Richtlinie „KISTERS Passwortrichtlinie“ festgelegt, die ebenfalls obligatorischer Bestandteil dieser Richtlinie ist.

3.3 Zugriffskontrolle

3.3.1 Interne und Vertrauliche Information

Die Klassifizierung von Daten und Informationen MUSS durch die Verantwortlichen für diese Daten und Informationen erfolgen.
Alle Daten und Informationen, auf die Mitarbeiter im Rahmen ihrer Tätigkeit bei der KISTERS Gruppe Zugriff erhalten, MÜSSEN – sofern nicht anders gekennzeichnet, als intern behandelt werden. Alle Daten, die unmittelbar oder mittelbar einer natürlichen Person zuzuordnen sind, unterliegen dem besonderen Schutz im Sinne der Europäischen Datenschutz-Grundverordnung (DS-GVO), des Bundesdatenschutzgesetzes (BDSG) und aller weiteren anwendbaren Datenschutzgesetze und MÜSSEN daher als vertraulich behandelt werden.
Im Umgang mit interner und vertraulicher Information jeglicher Art und in jeglicher Form sind folgende Regeln zu beachten:

- Die Information DARF NUR zu betrieblichen Zwecken genutzt werden.
- Die Information DARF NUR an berechtigte Empfänger (intern/extern) weitergegeben werden.
    - Die Information MUSS durch die Verantwortlichen zur Weitergabe freigegeben werden.
    - Die Berechtigung der Empfänger MUSS durch den Weitergebenden geprüft/verifiziert werden.
- Die Information MUSS vor unberechtigtem Zugriff geschützt werden.

3.3.2 Geschäftsdaten Dritter

Geschäftsdaten Dritter MÜSSEN immer als „vertraulich“ behandelt werden, sofern sie nicht durch die übergebenden Dritten anders klassifiziert sind.
Grundsätzlich MÜSSEN alle Daten, die uns von Kunden oder Partnern übergeben werden, von den entsprechenden Projektleitern verwaltet werden. Diese MÜSSEN auch diesbezügliche Nutzungsbedingungen des Kunden einhalten.
Die Projektleiter MÜSSEN über den korrekten Umgang mit diesen Daten wachen und haben die Pflicht, die mit diesen Daten in Berührung kommenden Personen auf die Einhaltung der jeweiligen Datenschutzrichtlinien hinzuweisen.
Es SOLL eindeutig nachvollziehbar sein, wer mit welchen Daten zu tun hat.

[INFO] Falls keine vom Kunden oder Partnern vorgegebenen Datenschutzbestimmungen vorliegen, so greifen in jedem Fall die KISTERS Informationssicherheitsrichtlinien sowie die Verpflichtungserklärung auf Geheimhaltung und Datenschutz der KISTERS Gruppe.

3.4 Aufgeräumter Arbeitsplatz - leerer Bildschirm

Der Grundsatz des leeren/aufgeräumten Schreibtisches und des leeren Bildschirms („clean desk – clear screen“) MUSS von jedem Mitarbeiter umgesetzt werden, um das Risiko eines unbefugten Zugangs und Zugriffs, den Verlust oder der Beschädigung von Unterlagen, Informationsträgern und informationsverarbeitenden Einrichtungen zu verringern.

3.4.1 Aufgeräumter Arbeitsplatz

Alle vertraulichen Unterlagen und Datenträger mit vertraulichem Inhalt DÜRFEN NUR solange am Arbeitsplatz aufbewahrt werden, wie es unbedingt erforderlich ist, um die damit verbundenen fachlichen Aufgaben zu erledigen. Ansonsten MÜSSEN diese Unterlagen jederzeit gesichert in verschlossenen Räumen oder Schränken deponiert werden. Besonders sensitive oder kritische Unterlagen (z.B. Personalunterlagen) MÜSSEN jederzeit in dafür vorgesehenen abgeschlossenen Räumen oder Schränken mit eingeschränkter Zutritts- bzw. Zugangsberechtigung untergebracht werden.

3.4.2 Leerer Bildschirm

Zur Vermeidung von unberechtigter Nutzung MUSS jedes Rechnersystem über einen aktivierten Sperrbildschirm mit Kennwortschutz verfügen. Bei jedem Verlassen des Arbeitsplatzes - auch für kurze Zeit - MÜSSEN Benutzer in jedem Fall den passwortgeschützten Sperrbildschirm aktivieren. Wenn eine Unterbrechung der Arbeit für mehr als einen Tag erwartet oder geplant ist, SOLLEN sich Benutzer von Einzelplatzsystemen (Workstations, Laptops, etc.) vom System abmelden. Benutzer MÜSSEN sich in jedem Fall bei einer Unterbrechung von mehr als einer Woche von Einzelplatzsystemen abmelden. Benutzer von Mehrbenutzersystemen MÜSSEN sich immer nach Erledigung der dort zu verrichtenden Aufgabe vom System abmelden.

3.5 Maßnahmen beim Verdacht auf unberechtigte Nutzung

Wenn der Verdacht besteht, dass ein Rechner oder eine Anwendung unberechtigt benutzt wurde oder dass auf Information ohne entsprechende Berechtigung zugegriffen wurde, SOLLEN folgende Schritte unternommen werden:

1. Ruhe bewahren! Auf gar keinen Fall sind auf dem Bildschirm ausgegebene Meldungen zu befolgen. Oftmals werden durch voreilige Reaktionen mögliche Spuren der unberechtigten Benutzung gelöscht und machen eine Nachverfolgung unmöglich.
2. Falls auf dem Bildschirm Hinweise auf die unberechtigte Nutzung oder den unberechtigten Zugriff zu finden sind, diese per Foto oder ggfs. Screenshot festhalten.
3. Falls Dateien oder Dateiinhalte auf unberechtigte Benutzung schließen lassen, diese nicht modifizieren oder löschen, sondern wenn möglich deren relevante Meta-Information (Ordnerpfad, Größe, Datum, etc.) notieren.
4. Die IT-Administratoren telefonisch(!) informieren. Dabei folgende Informationen bereithalten:
   4.1. Um welches Gerät handelt es sich, wo befindet es sich und wie ist es aktuell ins Firmennetzwerk eingebunden?

4.2. Wodurch ist die unberechtigte Nutzung bemerkt worden (ggf. Meldungen von Anwendungen, ungewöhnliche Prozesse, auffällige Dateien oder Dateiänderungen, etc.)
4.3. Welche Anwendungen waren in Benutzung und sind möglicherweise betroffen?
4.4. Welche Daten sind eventuell betroffen?
4.5. Auf weitere Anweisungen des IT-Administrators warten.

5. Zur weiteren Beweissicherung und ggfs. weiterer forensischer Untersuchung durch externe Spezialisten den Rechner umgehend nach Anweisung an die IT-Administration übergeben.

4 Datenschutz

[INFO] Datenschutz bezieht sich auf den Schutz von personenbezogenen Daten. Personenbezogene Daten sind alle Informationen, die sich auf eine bereits identifizierte oder durch die Information identifizierbare natürliche Person beziehen. Dazu gehören beispielsweise Name, Adresse und Geburtsdatum aber auch Standortdaten oder IP-Adressen, sofern diese (durch die Hinzunahme weiterer Informationen) einer Person zugeordnet werden können.
[INFO] Datenschutz bei der KISTERS Gruppe ist über die „Verpflichtungserklärung zu Informationssicherheit, Geheimhaltung und Datenschutz" geregelt. Die Verpflichtungserklärung wird von allen KISTERS Mitarbeitern unterzeichnet und ist Bestandteil des Anstellungsvertrages aller Angestellten der KISTERS Gruppe. Ein Verstoß gegen die Vorschriften aus dem Bereich Informationssicherheit, Geheimhaltung und Datenschutz wird disziplinarisch und (straf-)rechtlich im Rahmen der gesetzlichen Möglichkeiten verfolgt und geahndet.
Externe Mitarbeiter, die im Rahmen eines Projektes, Dienstleistungsauftrags o.ä. bei der KISTERS Gruppe oder für die KISTERS Gruppe tätig sind, MÜSSEN ebenfalls die „Verpflichtungserklärung zu Informationssicherheit, Geheimhaltung und Datenschutz" unterzeichnen. Für die Einholung der Unterschriften ist der jeweilige Projektleiter verantwortlich.

5 Datensicherung und -Archivierung

5.1 Datensicherung

[INFO] Die Datensicherung dient zur Vermeidung von möglichen Datenverlusten durch das regelmäßige Kopieren von Daten auf andere Datenträger (Backup). Diese Sicherungskopien können im Falle von Verlust oder Zerstörung der Originaldaten zu deren Wiederherstellung verwendet werden (Restore). Daten auf File-, Exchange- und Notes-Servern werden zentral täglich von der IT-Administration gesichert.
Für die Sicherung von lokal abgelegten Daten ist jeder Mitarbeiter selbst verantwortlich. Diese Daten SOLLEN regelmäßig durch die Mitarbeiter gesichert werden. Dazu stellt die IT-Administration geeignete Werkzeuge (Hardware/Software) zur Verfügung.
Weitere Regelungen zur Datensicherung sind in der „KISTERS IS Richtlinie für Administratoren" festgehalten.

5.2 Datenarchivierung

[INFO] Alle Geschäftsunterlagen und -daten unterliegen längerfristigen Aufbewahrungspflichten und Löschfristen aufgrund gesetzlicher Vorgaben. Die Datenbestände auf File-, Exchange - und Notes-Servern

werden zentral von der IT-Administration archiviert. Die Datenarchive werden nach Ablauf der Aufbewahrungsfristen gelöscht.
Daher MÜSSEN alle Mitarbeiter sämtliche geschäftsrelevanten Daten, wie z.B. Projektdaten, Vertragsdaten etc., auf den entsprechenden File-, Exchange- und Notes-Servern ablegen.

6 Verschlüsselung

Sensitive und kritische Daten unterliegen einem besonderen Schutzbedürfnis hinsichtlich ihrer Vertraulichkeit und DÜRFEN unter Umständen NUR verschlüsselt gespeichert oder übermittelt werden. Die Notwendigkeit der Verschlüsselung MUSS von den Verantwortlichen für diese Information festgestellt werden. Im Falle von personenbezogenen Daten SOLL der Datenschutzbeauftragte konsultiert werden.
Im Einzelnen sind die Vorgaben für die Verschlüsselung von Daten in der Richtlinie „KISTERS IS Leit- und Richtlinie zu kryptographischen Maßnahmen" festgelegt und sind obligatorischer Bestandteil dieser Richtlinie.
Im Folgenden sind die dort beschriebenen Maßnahmen in vereinfachter Form zusammengefasst.

6.1 Interne E-Mail

Interne E-Mails können in Outlook nicht verschlüsselt werden. Stattdessen MÜSSEN alle internen E-Mails, die vertrauliche Daten und Informationen enthalten (etwa Details zu Personaldaten) mit der Vertraulichkeit „**Privat**" versandt werden.

6.2 Externe E-Mail

Vertrauliche Informationen, die per E-Mail mit Externen (Kunden oder Partnern) ausgetauscht werden, SOLLEN verschlüsselt werden. Das Verfahren MUSS im Einzelfall mit dem externen Sender/Empfänger und der IT-Administration abgestimmt werden. Das Standardverfahren SOLL ein Austausch über S/MIME-Verschlüsselung sein.

6.3 Mobile Datenträger

[INFO] Mobile Datenträger sind u.a.

- alle USB-Flash Speicher (USB-Memory Sticks), SIM-Karten oder externe Festplatten, die per USB oder andere externe Ports an Rechnersysteme angeschlossen werden können,
- die Festplatten aller mobilen Arbeitsplätze wie Notebooks, Netbooks oder PDAs,
- Bänder, CDs, DVDs die zur Datensicherung und –archivierung verwendet werden.

Vertrauliche Daten MÜSSEN verschlüsselt auf diesen mobilen Datenträgern abgelegt werden.
[INFO] Der Datenträger wird entweder vollständig verschlüsselt (z.B. mittels BitLocker), oder es wird ein verschlüsselter Bereich auf dem Datenträger zur Speicherung vertraulicher Informationen angelegt (z.B. mittels VeraCrypt). Die für die Verschlüsselung notwendige Software, die die Verschlüsselung nach Stand der Technik (derzeit: AES-XTS-256) durchführt, wird von der Systemadministration zur Verfügung gestellt.
Alternativ KANN die Verschlüsselung auf einzelne Dateien oder Dateiarchive vertraulicher Daten angewendet werden. Dies KANN z.B. mit dem freien Verschlüsselungstool PDFEncrypt für PDF-Dateien oder dem Datei-Archivierungstool 7-zip durchgeführt werden. Bei der Verschlüsselung MUSS das Verfahren AES-256 angewendet werden, wenn das Tool dieses anbietet. In jedem Fall MUSS ein starkes Passwort gewählt werden.

Bei Verlust oder Diebstahl eines Datenträgers MUSS sofort die zentrale IT-Administration in Aachen informiert werden!

7 Beschaffung und Entsorgung von Datenträgern

IT-Systeme (Workstations, Laptops, Tablets, Mobiltelefone) und mobile Datenträger (Festplatten, USB-Sticks, Bänder, CDs, DVDs, etc.), die dienstlich genutzt werden oder auf denen dienstliche Daten (KISTERS Daten, Kundendaten) gespeichert werden, MÜSSEN von der KISTERS IT-Administration beschafft werden. Die dienstliche Nutzung von anderweitig beschafften Geräten ist VERBOTEN.
IT-Systeme und mobile Datenträger, die beschädigt sind oder nicht mehr benötigt werden, MÜSSEN zur Vorbereitung der Wiederwendung oder Entsorgung an die IT-Administration übergeben werden.
Auf diesen Geräten gespeicherte Daten, die nicht mehr benötigt werden, SOLLEN vor Abgabe der Geräte an die IT-Administration gelöscht werden, sofern dies technisch möglich ist.
[INFO] Die IT-Administration stellt sicher, dass vertrauliche Daten und lizensierte Software entfernt oder sicher überschrieben werden. Eine anderweitige Wiederverwendung oder Entsorgung ist nicht zulässig.
Weitere Regelungen zur Entsorgung von Datenträgern sind in der „KISTERS Informationssicherheitsrichtlinie für Administratoren“ festgehalten.
Nicht-elektronische Datenträger mit interner oder vertraulicher Information (z.B. handschriftliche Notizen, Ausdrucke u.ä.) MÜSSEN mit den an jedem Standort vorhandenen Aktenvernichtern vernichtet werden. Zur Vernichtung von größeren Mengen von Akten mit vertraulichen Daten SOLLEN diese in abgeschlossenen Behältern gesammelt und zur Vernichtung an einen spezialisierten Dienstleister übergeben werden.

8 Unternehmenswerte außerhalb von KISTERS Betriebsstätten

8.1 Allgemeine Regelungen

[INFO] Unternehmenswerte sind IT-Systeme, allgemeine Betriebsmittel, Information, Dokumente, Software etc., die zur Erfüllung der betrieblichen Aufgaben und zur Durchführung der Betriebsprozesse verwendet werden. Für Unternehmenswerte sind grundsätzlich folgende Regeln einzuhalten:

- Unternehmenswerte DÜRFEN NUR von sachkundigen und autorisierten Nutzern verwendet werden.
- Das Mitnehmen und die Nutzung von Unternehmenswerten außerhalb der KISTERS Betriebsstätten MUSS vom Verantwortlichen für diese Werte oder einem Vertreter autorisiert werden.
- Die Mitnahme von Unternehmenswerten SOLL dokumentiert werden, insbesondere wenn es sich um voraussichtlich längerfristige Entfernung der Werte aus den KISTERS Betriebsstätten handelt.
- Alle Unternehmenswerte MÜSSEN insbesondere außerhalb der KISTERS Betriebsstätten durch angemessene Maßnahmen gegen unbefugte Benutzung, Beschädigung, Entwendung und Verlust gesichert werden.
- Die Regelungen zur Zutritts-, Zugangs- und Zugriffskontrolle MÜSSEN jederzeit beachtet werden.
- Beim Transport von klassifizierten KISTERS-Dokumenten, IT-Systemen und anderen Werten zwischen KISTERS Standorten oder zwischen einem KISTERS Standort und Kunden, Partnern oder Dienstleistern MUSS die Vollständigkeit und Unversehrtheit der transportierten Werte bei der

Auslieferung überprüft werden. Dies KANN durch Erstellen und Überprüfen einer Teileliste oder einer Stückliste erfolgen.

- Diebstahl, Verlust oder unbefugter Nutzung von Unternehmenswerten sind Sicherheitsvorfälle und MÜSSEN den Verantwortlichen für diese Werte sowie dem CISO unverzüglich gemeldet werden.
- Nicht mehr benötigte Unternehmenswerte MÜSSEN an die zuständigen Verantwortlichen zurückgegeben werden.
- Vor der Rückgabe von nicht mehr benötigten IT-Systemen und Datenträgern an die IT-Administration SOLLEN alle internen und vertraulichen Daten gelöscht werden.

8.2 Mobile Nutzung von IT-Systemen, Telearbeitsplätze

[INFO] Mobile Geräte und Geräte von Telearbeitsplätzen werden regelmäßig außerhalb der zugangsgesicherten Betriebsstätten der KISTERS Gruppe transportiert, gelagert und genutzt. Die Geräte werden oft für den Zugriff auf andere KISTERS IT-Systeme und Information verwendet. Zur mobilen Nutzung gehört ebenfalls der Einsatz von IT-Systemen als Präsentations- oder Demosysteme auf Messen, Ausstellungen oder ähnlichen Veranstaltungen oder als Testsysteme bei Kunden oder Partnern. Für diese Geräte müssen besondere Maßnahmen gegen unbefugte Benutzung, Entwendung und Verlust ergriffen werden:

- Mobile Geräte und Telearbeitsplätze MÜSSEN jederzeit eindeutig einem Mitarbeiter zugeordnet sein.
- Mobile Geräte und Telearbeitsplätze MÜSSEN durch Passwörter und/oder PINs („Personal Identification Number“) vor unberechtigtem Zugang gesichert werden. Die Verwendung von Passwörtern und PINs ist in der Richtlinie „KISTERS Passwortrichtlinie“ festgelegt, die ebenfalls obligatorischer Bestandteil dieser „KISTERS Informationssicherheitsrichtlinie“ ist.
- Bei Verlust, Diebstahl oder Verdacht auf unbefugte Benutzung von mobilen Geräten oder Geräten von Telearbeitsplätzen MUSS sofort die zentrale IT-Administration in Aachen und der CISO informiert werden!
- Zur Weiterverwendung oder Entsorgung MÜSSEN alle mobilen Geräte und Geräte von Telearbeitsplätzen, die nicht mehr benötigt werden, an die zentrale IT-Administration zurückgegeben werden.
- Für mobile Geräte und Telearbeitsplätze MÜSSEN die Maßnahmen für mobile Datenträger, die Maßnahmen zum Schutz vor Schadsoftware, die Maßnahmen zur Datensicherung und die Maßnahmen für Fernzugänge beachtet werden.

8.2.1 Mobile Geräte

[INFO] Mobile Geräte sind u.a. Laptops, Notebooks, Netbooks, Tablets, PDAs, Smartphones, Kameras usw.

- Betrieblich genutzte mobile Geräte MÜSSEN von der IT-Administration beschafft und zur Nutzung freigegeben werden ("Firmengeräte").
- Die Geräte MÜSSEN jederzeit physikalisch gegen unbefugten Zugang, Verlust und Entwendung gesichert werden, z.B. durch
    - Persönliche Beaufsichtigung und Zugangssicherung (z.B. in Auto, Bahn, Flugzeug, …)
    - Aufbewahrung in verschlossenen Räumen oder Schränken
    - Anketten („Kensington Lock“)
- Für diese Geräte SOLL ein „boot-Kennwort“ vergeben werden.

- Die Benutzer MÜSSEN sicherstellen, dass die mobilen Geräte regelmäßig auf den neuesten Stand der IT-Sicherheit gebracht werden. Dazu gehören u.a. Sicherheitspatches der installierten Software sowie Updates von Virensignaturen. Dies MUSS, je nach Gerät, durch Anbindung an das KISTERS Netzwerk oder Übergabe des Geräts an die IT-Administration geschehen.
- Vertrauliche Daten MÜSSEN verschlüsselt auf den Datenträgern des mobilen Geräts abgelegt werden. Auf diesen Datenträgern SOLLEN NUR die für den Bestimmungszweck notwendigen vertraulichen Daten gespeichert werden.
  [INFO] Die für die Verschlüsselung notwendige Software stellt die IT-Administration zur Verfügung (s. Abschnitt „Mobile Datenträger“).
- Bei Verwendung von mobilen Geräten in privaten oder öffentlichen Netzwerken MUSS der Benutzer bei der Verbindung zum Netzwerk die entsprechenden Sicherheitseinstellungen wählen. Dazu gehören
  - Nutzung eines „Gäste-WLANs“ im Fall von drahtloser Verbindung
  - Netzwerkoption "Öffentlich", um eine Freigabe von Dateien zu verhindern
  - Verschlüsselung von Datenübertragungen durch Nutzung von VPN, https, sftp usw.
- Kommunikationsschnittstellen von mobilen Geräten wie Wi-Fi, Bluetooth oder NFC MÜSSEN deaktiviert werden, wenn keine Netzwerkverbindung benötigt wird. Datenverbindungen zwischen mobilen Geräten (z.B. über Bluetooth-Pairing) SOLLEN so selten wie möglich und idealerweise nur in physikalisch sicheren Umgebungen genutzt werden, in denen ein Mithören der Kommunikation durch unbefugte Dritte nicht möglich ist.
- Sprachassistenten SOLLEN deaktiviert werden, es sei denn sie werden zwingend benötigt. Generell SOLL ein Sprachassistent nicht genutzt werden können, wenn das Gerät gesperrt ist.
- Bei der Arbeit mit mobilen Geräten SOLL darauf geachtet werden, dass keine schützenswerten Informationen ausgespäht werden können. Dazu SOLL ein angemessener Sichtschutz verwendet werden, der den gesamten Bildschirm des jeweiligen Gerätes umfasst und ein Ausspähen von Informationen erschwert.

8.2.2 Smartphones

Für Smartphones gelten zusätzlich folgende Maßnahmen:

- Auf Smartphones DÜRFEN KEINE vertraulichen Daten gespeichert werden, mit Ausnahme einer verschlüsselten Kopie der persönlichen Outlook Datenbank.
- Smartphones, die nicht in Benutzung sind, MÜSSEN immer mit gesperrter Bedienfläche und gesperrtem Bildschirm (Display-Sperre) abgelegt werden.
- Die Entsperrung von Smartphones
  - MUSS mittels einer PIN oder eines biometrischen Verfahrens (Fingerabdruck, Gesichtserkennung) erfolgen;
  - über ein Entsperrmuster MUSS deaktiviert werden, da diese Muster leicht erkennbar sind.
- Auf dienstlich genutzten Smartphones DÜRFEN NUR bekannte und weit verbreitete Apps aus den offiziellen Stores installiert werden. Im Zweifelsfall SOLL eine Freigabe beim CISO-Team oder den SysAdmins eingeholt werden.
- Für Android Smartphones ist die Nutzung eines Antivirenschutzes empfohlen, aber nicht zwingend.

[INFO] Der Zugriff auf dienstliche Emails und den Kalender auf dem KISTERS Exchange Online Server (M365) von einem mobilen Gerät mittels Outlook App oder Web-Zugriff ist erlaubt und erfordert keine explizite Freigabe dieses Gerätes durch die Systemadministration. Der Datenaustausch zwischen Smartphone und Exchange Server erfolgt über eine verschlüsselte Internetverbindung. Alle lokalen Outlook-Daten MÜSSEN verschlüsselt auf dem Smartphone abgelegt werden.

8.2.3 Telearbeitsplätze

[INFO] Telearbeitsplätze sind Arbeitsplätze, die von KISTERS Mitarbeitern regelmäßig außerhalb der Betriebsstätten der KISTERS Gruppe genutzt werden (z.B. Homeoffice, temporärer Arbeitsplatz bei Kunden, Arbeiten unterwegs, …). Für Telearbeitsplätze stellt KISTERS den Mitarbeitern mobile oder stationäre Firmengeräte zur Verfügung, für die folgende Regelungen gelten:

- Die von KISTERS zur Verfügung gestellten Arbeitsmittel DÜRFEN NICHT für private Zwecke genutzt werden.
- Dir Arbeitsmittel DÜRFEN NICHT an Dritte überlassen werden.
- Die Mitarbeiter MÜSSEN dafür Sorge zu tragen, dass die Arbeitsmittel jederzeit physikalisch gegen unbefugten Zugang, Verlust und Entwendung durch Dritte geschützt sind.
- Die betrieblichen und gesetzlichen Regelungen des Datenschutzes und der Datensicherheit MÜSSEN beachtet und angewendet werden.
- Insbesondere MÜSSEN die Vorgaben zum aufgeräumten Arbeitsplatz und leeren Bildschirm beachtet werden.
- Interne und vertrauliche Information MUSS von den Mitarbeitern so geschützt werden, dass Dritte - insbesondere auch im Haushalt der Mitarbeiter lebende Personen - keine Einsicht und/oder keinen Zugriff nehmen können.
- Dokumente oder Datenträger DÜRFEN NUR mit Zustimmung des Vorgesetzten an den Telearbeitsplatz gebracht werden und MÜSSEN verschlüsselt oder in verschlossenen Behältnissen transportiert werden.
- Für Homeoffices: Der Internetzugang der dienstlichen IT-Systeme SOLLTE vom Heimnetzwerk getrennt sein, z.B. durch Nutzung eines separaten Gastzugangs. Falls dies nicht möglich ist, MUSS der Zugang zum Heimnetzwerk als Zugang zu einem „öffentlichen Netzwerk“ konfiguriert werden.
- Für den Zugang zum KISTERS Netzwerk MÜSSEN die von der IT-Administration zur Verfügung gestellten VPN-Software und Zugangsdaten verwendet werden.

Weitere spezifische Maßnahmen für die Einrichtung und Nutzung von Telearbeitsplätzen sind in der „KISTERS Vereinbarung zur Telearbeit“ festgelegt.

9 Private Geräte und Medien - „Restricted BYOD“-Richtlinie

Geräte und Medien (stationäre oder mobile IT-Systeme, Datenträger, Peripheriegeräte, etc.), die im Privateigentum von KISTERS Mitarbeitern sind, DÜRFEN im Ausnahmefall dienstlich für zeitlich begrenzte oder funktional eingeschränkte Aufgaben verwendet werden („eingeschränkte Nutzung von privaten Geräten“, „Restricted Bring Your Own Device“).

- Die Nutzung MUSS vorher vom Vorgesetzten des Mitarbeiters genehmigt werden; in Ausnahmefällen (z.B. Notfallsituationen) KANN die Nutzung auch nachträglich genehmigt werden.

- Eine Genehmigung DARF NUR erteilt werden, wenn die Geräte und Medien einen für die vorgesehene Verwendung ausreichenden Sicherheitsstand aufweisen (z.B. aktuelles Antivirus-Programm auf IT-Systemen, gesicherter physischer Zugangsschutz und Virencheck für Datenträger).
- Auf privaten Geräten DÜRFEN KEINE vertraulichen Daten gespeichert werden. Sollten dennoch im Ausnahmefall vertrauliche Information auf privaten Geräten gespeichert werden (z.B. Notizen, Fotos von Whiteboards oder Bildschirmen, etc.), so MUSS diese schnellstmöglich von den Geräten entfernt/gelöscht werden.
- Ist in diesem Zusammenhang die Übertragung von Daten von einem privaten Gerät auf ein KISTERS IT-System notwendig, dann MÜSSEN die gleichen Vorsichtsmaßnahmen angewendet werden wie bei einer Übertragung von Daten aus dem Internet oder anderen ungesicherten Quellen.

9.1 Betriebliche Cloud-Dienste auf privaten Geräten

[INFO] Es ist technisch nicht möglich, die Nutzung von betrieblich Cloud-Diensten wie Outlook, Teams oder Confluence und Jira von privaten IT-Systemen (Smartphones, Tablets, Laptops etc.) zu verhindern. Diese Dienste verlangen eine 2-Faktor-Authentisierung, so dass eine missbräuchliche unautorisierte Nutzung erschwert wird. Allerdings können je nach genutztem Benutzer-Interface (Web, App) bei der Nutzung bewusst oder automatisch Daten lokal auf den privaten IT-Systemen gespeichert werden. Daher sind folgende Regeln zur Nutzung dieser Dienste auf privaten IT-Systemen zu beachten:

- Die Nutzung der betrieblichen Cloud-Dienste DARF NUR dann von privaten IT-Systemen vorgenommen werden, wenn es dafür eine betriebliche Notwendigkeit gibt.
- Private IT-Systeme, mit denen auf betriebliche Cloud-Dienste zugegriffen wird, MÜSSEN bezüglich ihrer IT-Sicherheit wie dienstliche IT-Systeme behandelt werden (Zugangsschutz, Virenschutz, Patchmanagement, etc.). Die Verantwortung dafür tragen die Nutzer.
- Wenn die Nutzung nicht mehr benötigt wird, z.B. beim Ausscheiden aus dem Unternehmen, MÜSSEN alle dienstlichen Daten (z.B. E-Mail), die aufgrund der Nutzung der Cloud-Dienste auf den privaten IT-Systemen gespeichert wurden, vollständig gelöscht werden.
- Falls es aufgrund der Nutzung von betrieblichen Cloud-Diensten auf privaten IT-Systemen zu Sicherheitsrisiken kommt, so KANN diese Nutzung individuell per Dienstanweisung untersagt werden. Zuwiderhandlungen werden entsprechend geahndet.

10 Netzwerkzugänge

[INFO] Das KISTERS Netzwerk ist logisch in verschiedene Segmente separiert, die für unterschiedliche Zwecke genutzt werden und unterschiedlichen Schutzbedarf haben:

- Allgemeines KISTERS Datennetz (KISTERS LAN, „wlanac22“)
- Netzwerk zum Zugriff auf das Internet für mobile KISTERS Geräte und Smartphones („mnotes“)
- Netzwerk zum Zugriff auf das Internet für externe Dritte (Besucher, Dienstleister etc.) („External-Guests“)
- Spezielle Netzwerke mit besonderen Zugriffsberechtigungen (administrativer Zugriff auf IT-Systeme, Netzwerk zur Datensicherung, KISTERScloud-Netzwerk, …)

10.1 Zugang ins KISTERS Datennetz

[INFO] Der Zugang zum firmenweiten Datennetz aus dem Internet ist ausschließlich über den OpenVPN Client bzw. Cisco VPN (bei älteren Systemen) realisiert. Zugangskennungen werden, nach vorheriger Prüfung, nur personenbezogen und nur von der zentralen IT-Administration in Aachen vergeben.
Für den Zugang ins Datennetz DÜRFEN NUR Geräte verwendet werden, die von der zentralen IT-Administration in Aachen dafür freigegeben werden und ausschließlich dienstlich genutzt werden. In der Regel handelt es sich dabei um Firmenrechner; private IT-Systeme (Rechner, mobile Geräte) sind vom Zugang zum Firmennetz ausgeschlossen. Smartphones sind ebenfalls vom Zugang zum Datennetz ausgeschlossen.
In besonderen Fällen KANN der Vorstand der KISTERS AG eine Ausnahmegenehmigung für den Zugang zum Firmennetz von KISTERS Mitarbeitern über private Rechner unter weiteren Auflagen erteilen.

10.2 Zugang zum Internet

[INFO] Der Zugang zum Internet ist für Geräte, die keine Verbindung zum KISTERS Datennetz haben, nur über das „mnotes“-Netzwerk möglich. Dies betrifft insbesondere alle Smartphones, die zum Zugriff auf die dienstliche E-Mail des Benutzers über Outlook freigegeben sind, unabhängig davon, ob es sich um Firmengeräte oder private Geräte von KISTERS Mitarbeitern handelt. Aufgrund der Netzwerksegmentierung ist der Zugriff auf das Datennetz über Smartphones nicht möglich. Die Nutzung des „mnotes“-Netzwerks ist für Externe Dritte nicht gestattet.

10.3 Zugang zum Internet für Externe

[INFO] Innerhalb der KISTERS Betriebsstätten können Externe von ihren Geräten aus nur über WLAN („ExternalGuests“) auf das Internet zugreifen.
Dazu MÜSSEN temporär gültige Passwörter bei der IT-Administration beantragt werden.

10.4 Zugänge zu externen Systemen / Fernwartungszugänge

[INFO] Zugänge zu externen IT-Systemen (Fernwartungszugänge, Zugänge zu IT-Systemen von Kunden oder Partnern) werden zentral von der IT-Administration in Aachen verwaltet. Dazu stellt die IT-Administration spezielle Rechner (Virtuelle Maschinen) zur Verfügung, die für den Zugriff auf spezifische Kundensysteme konfiguriert sind und in separaten Subnetzen liegen.

- Zugriffe auf Kundensysteme DÜRFEN NICHT direkt von Arbeitsplatzrechnern, sondern NUR über diese von der IT-Administration bereitgestellten Systeme durchgeführt werden.
- In Ausnahmefällen KÖNNEN Zugriffe von Arbeitsplatzrechnern mittels TeamViewer durchgeführt werden, dazu MUSS die explizite Zustimmung der Kunden oder Partner eingeholt werden.
- Die Nutzer eines Fernwartungszuganges MÜSSEN benannt werden. Ein Fernwartungszugang DARF NUR von den Personen genutzt werden, die dem Kunden/Partner benannt wurden.
- Während der Fernwartungsarbeiten MÜSSEN unbedingt die Sicherheits- und Datenschutzbestimmungen des Kunden beachtet werden. Bei Bedarf MÜSSEN diese Informationen vor Beginn der Arbeiten eingeholt werden.
- Mitarbeiter, die Fernwartungszugänge genutzt haben und aus der KISTERS Gruppe ausscheiden, MÜSSEN dem Kunden benannt werden. Der Kunde SOLL dann entscheiden, ob neue Zugangsdaten erstellt werden oder die bestehenden weiter genutzt werden können.
- Zugangskennungen DÜRFEN NUR autorisierten Personen zugänglich gemacht werden.

Im Übrigen gelten die Vorgaben für die Behandlung von Passwörtern und die Sicherung des Zugangs auf die dafür vorgesehenen Systeme (Abmeldung, Sperrbildschirm, etc.) entsprechend.

10.4.1 Verbot der privaten Nutzung

Alle IT-Komponenten, von denen ein Zugriff auf IT-Systeme von Kunden oder Partnern möglich ist, DÜRFEN NUR für dienstliche Zwecke genutzt werden. Eine private Nutzung durch die Mitarbeiter ist VERBOTEN. Private IT-Komponenten DÜRFEN NICHT für den Zugriff auf Systeme von Kunden oder Partnern benutzt werden bzw. nicht an IT-Systeme angeschlossen werden, die für den Zugriff auf Ressourcen der Kunden/Partner vorgesehen sind.

11 E-Mail, Internet, Kommunikationssoftware und KI-Assistenzsysteme

11.1 E-Mail

Die betrieblichen E-Mailadressen und -Postfächer werden den Mitarbeitern der KISTERS Gruppe als Arbeitsmittel zur Verfügung gestellt und DÜRFEN NUR betrieblich genutzt werden, eine private Nutzung ist nicht erlaubt. Die betriebliche Nutzung umfasst

- die interne Kommunikation innerhalb der KISTERS Gruppe,
- die externe Kommunikation mit externen Dritten (Kunden, Partnern, Zulieferern etc.) für betriebliche Zwecke,
- die Anmeldung bei Foren, Webseiten, Serviceportalen, Lieferanten, Ausschreibungsplattformen etc. für betriebliche Zwecke,
- die „betrieblich veranlasste Privatnutzung“ (z.B. Mitteilung an Familienmitglieder, dass sich die Heimkehr verzögert),
- die Förderung des Privatkontaktes zu Kunden, soweit dies unmittelbar von betrieblichem Interesse ist.

Nicht erlaubt sind unter anderem

- die private Kommunikation mit externen Dritten,
- die Anmeldung an Foren, Webseiten, Serviceportale, Online-Shops, Social Media etc. für private Zwecke,
- die Nutzung des Outlook-Clients auf KISTERS IT-Systemen zum Abruf von anderen, nicht betrieblichen E-Mail-Postfächern und Kalendern.

Automatische Weiterleitungen von E-Mails an externe E-Mailadressen DÜRFEN NICHT eingerichtet werden.

Alle ein- und ausgehenden E-Mails MÜSSEN unabhängig vom tatsächlichen Inhalt als geschäftliche/betriebliche Dokumente eingestuft werden und unterliegen den damit verbundenen Klassifikations-, Kontroll- und Archivierungsprozessen.

E-Mails haben rechtlich die Bedeutung eines geschriebenen Briefes und MÜSSEN klar den Absender erkennen lassen. Alle ausgehenden E-Mails MÜSSEN immer mit einer gültigen dienstlichen Signatur des Absenders versehen werden.

[INFO] Signaturen werden zentral an versendete Mails angehängt und sind zum Zeitpunkt des Versandes für den Nutzer nicht sichtbar. Information hierzu sind in KISTERS Confluence unter dem Suchbegriff „kisters mail signatur“ verfügbar.

11.2 Internet

Die Internetanbindung der KISTERS Gruppe ist der betrieblichen Nutzung vorbehalten. Eine private Nutzung der Internetanbindung der KISTERS Gruppe ist erlaubt, allerdings MÜSSEN die den nachstehenden Verhaltensregeln eingehalten werden:

- Die private Nutzung DARF NICHT den ordnungsgemäßen Geschäftsbetrieb beeinträchtigen, z.B. durch Herunterladen von großen Datenmengen.
- Es ist untersagt, Internetseiten zu besuchen bzw. Inhalte mit Dritten auszutauschen, die
    - erkennbar gegen Recht und Gesetz verstoßen,
    - pornographische Inhalte zur Verfügung stellen bzw. diese anbieten,
    - sexuell anstößig sind,
    - zum Rassenhass aufstacheln,
    - Gewalt verherrlichen oder verharmlosen,
    - den Krieg verherrlichen,
    - geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden oder in ihrem Wohl zu beeinträchtigen.
- Das Herunterladen von Spielen, Musik und Videos und anderen Inhalten, die aufgrund von Urheberrechten nicht heruntergeladen werden dürfen oder erkennbar geeignet sind, die Informationssicherheit zu gefährden, ist nicht gestattet.
- Die Vervielfältigung von Spielen, Musik, Videos und anderen urheberrechtlich geschützten Inhalten ist nicht gestattet.

Bei diesen Regeln handelt es sich um selbstverständliche Verhaltensformen. Sollten diese Verhaltensregeln nicht eingehalten werden, ist KISTERS gezwungen, die Internetnutzung personenbezogen komplett zu sperren. Falls der KISTERS Gruppe durch diese Aktivitäten materielle oder immaterielle Schäden entstehen, so werden weitere disziplinarische und (straf-)rechtliche Maßnahmen im Rahmen der gesetzlichen Möglichkeiten ergriffen.

11.3 Internet-basierte Anwendungen und Cloud-Dienste

Anwendungen, bei denen interne oder vertrauliche Daten aus dem Firmennetzwerk auf externe IT-Systeme ausgelagert oder repliziert werden, DÜRFEN NICHT ohne Freigabe durch den CISO benutzt werden. Dazu gehören u.a. Internet- bzw. Cloud-basierte Dienstprogramme und Desktop-Anwendungen (z.B. Google Desktop, DropBox, oder ähnliche), durch die Dokumente, Datei-Indizes oder -Kataloge oder andere Informationen und Daten auf externen IT-Systemen temporär oder permanent gespeichert werden. Ebenso gehören dazu Online-Dienste wie Dateikonverter, Übersetzer, oder Dienste auf Basis von künstlicher Intelligenz.
Anwendungen, die automatisch und vom Anwender unkontrolliert Dateien oder aktive Inhalte aus dem Internet auf KISTERS IT-Systeme laden, DÜRFEN NICHT installiert und benutzt werden.

Falls die Nutzung eines derartigen Systems aus Geschäftsgründen notwendig ist, MUSS die Nutzung durch die IT-Administration, den CISO und die Verantwortlichen für die betroffene Information genehmigt werden. Dabei MÜSSEN spezifische Regeln und Einschränkungen der Benutzung festgelegt werden. Die aktuelle Liste der freigegebenen Software und Dienste wird in Confluence gepflegt: „Software approved for communication and remote access".
Die Nutzung von internet-basierten Anwendungen, die von Kunden oder Partnern im Rahmen von gemeinsamen Projekt- oder Kooperationsarbeiten betrieben oder administriert werden (z.B. Trello, SharePoint, GitHub, etc.), MUSS durch die IT-Administration, den CISO und die Verantwortlichen für die betroffene Information genehmigt werden.
Eine Genehmigung MUSS widerrufen werden, wenn aufgrund von Sicherheitsvorfällen oder anderen Erkenntnissen die Informationssicherheit oder der Datenschutz bei der Nutzung der Anwendung nicht gewährleistet werden kann.

11.4 Kommunikations- und Steuerungssoftware

Softwareprodukte wie Microsoft Teams, Skype, TeamViewer, VNC und ähnliche DÜRFEN NUR dann für interne und externe Kommunikation verwendet werden, wenn sie durch die KISTERS IT-Administration freigegeben sind und gepflegt werden. Die aktuelle Liste der freigegebenen Software und Dienste wird in Confluence gepflegt: „Software approved for communication and remote access". Dabei MÜSSEN folgende Sicherheitsmaßnahmen beachtet werden:

- Passwort
    - Sofern die Authentifizierungsfunktion der Software nicht an den zentralen KISTERS Authentifizierungsserver (Active Directory) angeschlossen ist, MÜSSEN die Passwörter applikationsspezifisch sein und DÜRFEN NICHT für andere Applikationen und Systeme verwendet werden.
- Kontakte
    - Da in vielen Kommunikationstools (z.B. Skype) die Identität des Rufers (Versenders von Nachrichten) nicht gesichert ist, SOLLEN diese Tools nur zur Kommunikation mit bekannten und verifizierten Kommunikationspartnern genutzt werden.
    - Kommunikationstools SOLLEN so eingestellt sein, dass nur Kontakte aus der Kontaktliste anrufen dürfen.
    - Eingehende Anrufe DÜRFEN NICHT automatisch angenommen werden.
- Datenaustausch
    - Es DARF KEINE vertrauliche oder sensible Information (z.B. Passwörter) per Chat ausgetauscht werden.
    - Es DARF KEIN Transfer von Dateien mit vertraulichem oder sensiblem Inhalt erfolgen.
    - Der Empfang von Dateien DARF NUR von vertrauenswürdigen Kommunikationspartnern und nur mit aktivem und aktuellen Virenschutzprogramm erfolgen.
    - Bei der Übertragung von Bildschirminhalten MUSS sichergestellt sein, dass keine vertraulichen oder sensiblen Daten im übertragenen Video sichtbar sind.
    - Bei der Benutzung von Webcams bei Chats MUSS ebenfalls sichergestellt sein, dass keine vertraulichen oder sensiblen Daten im übertragenen Bildbereich sichtbar sind.
- Links

- Vor dem Anklicken von Internet-Links in Chats MÜSSEN diese auf Vertrauenswürdigkeit bzw. Korrektheit überprüft werden, um den Zugriff auf betrügerische oder gefährliche Webseiten weitgehend auszuschließen.
- Insbesondere MUSS die Vertrauenswürdigkeit von Internet-Links, die als Chat-Nachricht außerhalb einer aktiven Sitzung erhalten wurden, durch explizite Nachfrage beim angezeigten Sender über ein anderes Kommunikationsmittel (E-Mail, Telefon) überprüft werden.
- Wenn der angezeigte Sender die Authentizität der Chat-Nachricht nicht eindeutig bestätigt, dann DARF der Link NICHT angewählt werden, da der Account des Absenders sehr wahrscheinlich kompromittiert wurde.

- Fernsteuerung
  - Eine Fernsteuerung eines Rechners DARF NUR unter Aufsicht des Benutzers oder eines Administrators und DARF NUR durch vertrauenswürdige Partner erfolgen.
  - Die Software DARF NICHT im Hostmodus (unbeaufsichtigter Zugriff) betrieben werden, um einen unkontrollierten Fernzugriff auf den Rechner zu vermeiden.
- Kompromittierter Account
  - Besteht der Verdacht, dass ein Benutzer-Account kompromittiert wurde, dann MÜSSEN die IT-Administration und der CISO informiert werden. Darüber hinaus SOLL der Anwender versuchen, den Dienstleister des betroffenen Service zu informieren und den kompromittierten Account vollständig zu löschen, um jeglichen weiteren Missbrauch weitgehend auszuschließen.
- Software
  - Nicht freigegebene Software für Kommunikation, Dateitransfer, Fernzugriff oder Fernsteuerung von Rechnern (z.B. GoToMyPC, Dameware, Radmin, oder ähnliche) DARF NICHT installiert und genutzt werden.

11.5 Einsatz von KI-Assistenzsystemen

[INFO] KI-Assistenzsysteme oder auch AI-Assistenzsysteme sind Systeme, die auf künstlicher Intelligenz basieren und Menschen bei der Erledigung von Aufgaben oder der Beantwortung von Fragen unterstützen. Bekannte Beispiele von KI-Assistenzsystemen sind ChatGPT von OpenAi und Copilot von Microsoft. Auch die Sprachassistenten Siri, Google Assistant und Alexa sind ebenfalls bekannte Beispiele, die KI nutzen. KI-Assistenzsysteme bringen nicht nur einige Vorteile, sondern insbesondere beispielsweise Richtung Datenschutz bzw. Schutz von internen Informationen und Urheberrechten auch einige Risiken mit sich. Folgende Regeln sind daher zu beachten:

Es DÜRFEN ausschließlich freigegebene KI-Assistenzsysteme genutzt werden (siehe Confluence). In jedem Fall MUSS die „Corporate Policy on the Use of Artificial Intelligence Tools" zu beachten. Insbesondere bei öffentlichen KI-Systemen DÜRFEN KEINE personenbezogenen oder internen Firmendaten preisgegeben werden. Mitarbeiter SOLLEN im Umgang mit KI-Assistenzsystemen geschult werden, damit sie die Fähigkeiten, Einschränkungen und Risiken der Systeme verstehen. Mitarbeiter SOLLEN nicht blind auf deren Ergebnisse verlassen. Eigentum an Inhalten, die mit KI-Assistenzsystemen erstellt wurden, unterliegen den Richtlinien von KISTERS zum geistigen Eigentum. Die korrekte Zuordnung und Einhaltung des Urheberrechts sind unerlässlich.

12 Installation von Software

Die Installation von Software (Applikationsprogramme, Dienstprogramme, Treiber o.ä.) auf KISTERS IT-Systemen stellt eine administrative Aufgabe dar und DARF NICHT ohne entsprechende Berechtigung, Genehmigung, Kenntnisse und Vorsichtsmaßnahmen durchgeführt werden.
Vor der Installation der Software MUSS überprüft und sichergestellt werden, dass die Software den Anforderungen an Informationssicherheit und Datenschutz genügt, und dass die vorgesehene betriebliche Nutzung durch die Nutzungs- und Lizenzrechte gestattet ist.
Software, die auf Arbeitsplatzrechnern installiert werden soll, MUSS vorher von der IT-Administration oder dem CISO-Team zur Installation freigegeben und MUSS in die Liste der freigegebenen Software-Tools aufgenommen werden.
Software, die nicht von der IT-Administration installiert und gepflegt wird, MUSS in jedem Fall vom Systemverantwortlichen jederzeit aktuell gehalten werden; insbesondere MÜSSEN Sicherheitspatches bei Verfügbarkeit so schnell wie möglich installiert werden.
Weitere Regelungen dazu sind in der „KISTERS Informationssicherheitsrichtlinie für Administratoren und Systemverantwortliche“ erfasst.

13 Schutz vor Schadsoftware

[INFO] Schadsoftware wie Computerviren, Würmer, trojanische Pferde oder logische Bomben können auf verschiedensten Wegen in die KISTERS IT-Systeme gelangen. Es ist daher unabdingbar, dass alle IT-Anwender aktiv Maßnahmen ergreifen, eine Infektion durch oder Ausbreitung von Schadsoftware zu verhindern, und sich nicht nur auf die automatischen Virenscanner verlassen.

13.1 Maßnahmen gegen Schadsoftware (proaktiv)

Nachfolgende Anweisungen und Regeln sind unabhängig vom genutzten IT-System zu beachten. Die mit (*) gekennzeichneten Maßnahmen sind auf den Windows-Systemen, die von der IT-Administration eingerichtet und verwaltet werden, bereits durch Gruppenrichtlinien bzw. Konfiguration entsprechend eingerichtet und DÜRFEN NICHT durch Benutzer oder Administratoren außer Kraft gesetzt werden. Für alle anderen IT-Systeme MÜSSEN diese Maßnahmen durch die verantwortlichen Benutzer bzw. Administratoren entsprechend eingerichtet und eingehalten werden.

- Auf dem System MUSS ein aktueller Viruschecker installiert und aktiviert sein (*).
- Datenträger (USB-Sticks, SD-Karten, Disketten, CD/DVDs, mobile Festplatten, …) unbekannter oder zweifelhafter Herkunft DÜRFEN NICHT mit KISTERS IT-Systemen verbunden werden.
- Datenträger von vertrauenswürdigen Externen MÜSSEN vor dem ersten Lesezugriff mittels eines aktuellen Virencheckers auf Virenbefall überprüft werden (*).
- Die Festplatte MUSS regelmäßig mittels Virenchecker nach Viren durchsucht werden (*).
    - Hierzu SOLL die Funktion „Scan for Viruses“ des Explorer-Kontextmenü am entsprechenden Laufwerk verwendet werden.
- Die autorun-Funktion MUSS für alle Datenträger deaktiviert werden (*).
- In Dateiverwaltungsprogrammen, wie z.B. dem Windows Explorer, SOLL die Anzeige aller Dateitypen aktiviert werden. Dies kann die Entdeckung möglicher Computeranomalien erleichtern.

- Die Ausführung von Makros in Standardanwendungsprogrammen (z.B. Dokumente aus Textprogrammen, Tabellen und Mappen aus Tabellenkalkulationsprogrammen, Präsentationen aus Präsentationserstellungsprogrammen) SOLL standardmäßig deaktiviert werden. Dies gilt insbesondere für Dokumente, die aus dem Internet oder von Dritten via E-Mail oder anderen Datenaustauschmechanismen stammen. Makros SOLLEN nur dann aktiviert werden, wenn das Dokument aus vertrauenswürdiger Quelle stammt und der automatische Viruscheck nach dem Speichern keine Bedrohung identifiziert hat.
- [INFO] Eingehende E-Mails werden in erster Instanz durch den allgemeinen Spam-Filter überprüft und bei Verdacht auf schädlichem Inhalt in die „Quarantäne“ verschoben. Trotzdem kann es passieren, dass schädliche E-Mails nicht automatisch erkannt und isoliert werden. E-Mails können erfahrungsgemäß gefährlich sein, insbesondere wenn
    - der Absender nicht eindeutig verifizierbar ist,
    - der Text nicht zum Absender passt (z.B. englischer Text vom deutschen Freund),
    - der fehlende oder ein falscher Bezug zu vorausgegangenen Schreiben auffällt,
    - sie weitere Kopien zu unbekannten Adressaten aufweisen,
    - sie Links zu unbekannten oder zweifelhaften Webseiten enthalten,
    - sie zu dringenden Handlungen auffordern auch in Verbindung mit der Maßgabe zu strikter Vertraulichkeit,
    - mehrere Nachrichten mit gleichlautendem Betreff eingegangen sind,
    - diese unaufgefordert oder unangekündigt von unbekannten Absendern eintreffen,
    - Begriffe wie "Geld", "Sex", "Geheim" usw. in der Betreffzeile auftreten.

  E-Mails, die offensichtlich oder möglicherweise gefährlich sind, SOLLEN als Attachment an das Postfach „mailsecurity@kisters.de“ weitergeleitet und anschließend sofort gelöscht werden. Falls der Absender der Mail unbekannt ist, dann SOLL dieser Absender lokal gesperrt werden.
  Weiterhin gelten folgende Regeln:
    - Ausführbare Dateien (z.B. Programme, Skripte, Makros usw.) MÜSSEN immer erst lokal gespeichert werden und dürfen erst dann ausgeführt bzw. geöffnet werden.
    - Offensichtlich inkorrekte E-Mails oder „Spam-Mails“ (z.B. Werbung per E-Mail) SOLLEN ungeöffnet gelöscht werden.
    - Vor dem Anklicken von Internet-Links in E-Mails MÜSSEN diese soweit möglich auf Vertrauenswürdigkeit bzw. Korrektheit überprüft werden, um den Zugriff auf betrügerische oder gefährliche Webseiten weitgehend auszuschließen („Phishing Mails“). [INFO] Beim Positionieren der Maus über dem Text des Links erscheint am unteren Fensterrand die tatsächlich hinter dem Text verborgene Linkadresse. Die von uns eingesetzten E-Mail Spamfilter (Microsoft, Mimecast) bieten einen zusätzlichen Schutz vor gefährlichen Internet-Links, in dem sie in E-Mails von externen Absendern die ursprünglichen Linkadressen durch erweiterte oder automatisch generierte Links ersetzen (URL Rewriting). Beim Anklicken dieser ersetzten Links wird nicht direkt die ursprüngliche Linkadresse aufgerufen, sondern eine Sicherheitsüberprüfung vorgeschaltet. Eine Weiterleitung erfolgt nur, wenn die Spamfilter keine offensichtliche Bedrohung feststellen.

    - Vor dem Einscannen von QR-Codes MUSS ebenfalls die Vertrauenswürdigkeit bzw. Korrektheit des Absenders verifiziert werden, da die QR-Codes ebenfalls auf betrügerische oder gefährliche Webseiten verweisen können.
    - Angebliche externe Virenberichte SOLLEN NICHT per E-Mail weitergeschickt werden, da es sich in den meisten Fällen um Falschmeldungen (Hoaxes) handelt und die IT-Administration meist schon über aktuelle Viren informiert ist.
- [INFO] Auch Internet-Browser bieten einen gewissen Schutz gegen Viren. Hierfür müssen aber die Sicherheitseinstellungen des Browsers auf ein hohes Schutzniveau reguliert werden, damit aktive Inhalte (ActiveX, Java und JavaScript), die Viren enthalten können, deaktiviert sind. Da dies immer zu Behinderungen beim Surfverhalten führt - z.B. ständige Nachfragen, ob eine Seite wirklich geöffnet werden soll, aber auch die Weigerung, bestimmte Seiten zu öffnen -, werden diese Funktionen vom Hersteller standardmäßig deaktiviert. Dies bedeutet, dass die Browser eine Schutzwirkung nur dann entfalten, wenn der Benutzer vorher die Grundeinstellungen entsprechend angepasst hat.
- Das Herunterladen von Dateien aus dem Internet DARF NUR von vertrauenswürdigen Internetseiten geschehen, wie z.B. die Originalseiten von Software- und Hardwareherstellern, öffentlichen Institutionen, Partnern o.ä.
- Anwendungsprogramme, Treiber oder andere ausführbare Dateien DÜRFEN NUR unter Einhaltung der „KISTERS Informationssicherheitsrichtlinie für Administratoren“ aus dem Internet heruntergeladen und installiert werden.
- Anwendungsprogramme, für die KISTERS keine gültige kommerzielle oder „public domain“-Lizenz besitzt, DÜRFEN NICHT installiert werden.
- Anwendungsprogramme, die nicht von der Systemadministration beschafft und installiert werden, DÜRFEN NUR nach Prüfung und Freigabe durch den CISO heruntergeladen und installiert werden.
- Nicht mehr benötigte Anwendungsprogramme MÜSSEN in jedem Fall von den IT-Systemen entfernt werden.

[INFO] In den meisten Fällen wird ein Virus erst anhand seiner Auswirkungen und Schäden erkannt. Dazu gehören u.a.:

- Unnormales Verhalten des PC
- Unerwartete Verzögerungen beim Aufruf von Programmen und Daten
- Unerklärlicher Rückgang des verfügbaren Speicherplatzes im Arbeitsspeicher oder auf der Festplatte
- Auffällig lange Reaktionszeiten im Programmablauf
- Auffällig hohe CPU-, Platten- oder Netzwerk-Last ohne Benutzeraktivität
- Unerklärliche Systemabstürze in bisher einwandfrei laufenden Programmen
- Falsche oder veränderte Bildschirmdarstellung
- Veränderte oder fehlende Dateien bzw. Programme

[INFO] Falls man eine verdächtige Datei scannen möchte, bei der der installierte Virenscanner keine Bedrohung erkannt hat, ist dies z.B. bei diesen Seiten möglich:

- https://www.virustotal.com/gui/home/upload/
- https://internxt.com/virus-scanner/
- https://metadefender.opswat.com/
- https://www.hybrid-analysis.com/

Allerdings DÜRFEN KEINE datenschutzrelevanten vertraulichen Daten (Dateien mit Kundendaten, Passwörtern, etc.) dort zum Scannen hochgeladen werden!

13.2 Maßnahmen bei Verdacht auf Befall durch Schadsoftware (reaktiv)

Wenn der Verdacht besteht, dass ein Rechner von einem Virus befallen ist, SOLLEN folgende Schritte unternommen werden:

1. Ruhe bewahren!!! Auf gar keinen Fall sind auf dem Bildschirm ausgegebene Meldungen, z. B. Aufforderung zum Formatieren der Festplatte, zu befolgen. Oftmals wird durch panische Reaktionen ein größerer Schaden angerichtet als durch den Virus selbst.
2. Sofort alle Netzwerkverbindungen trennen: Flugzeugmodus aktivieren, WiFi/Bluetooth ausschalten, Netzwerkkabel ziehen. Insbesondere müssen alle Verbindungen zum KISTERS Netzwerk getrennt werden!
3. Keine Programme mehr starten und keine Dateien mehr öffnen.
4. Die IT-Administratoren MÜSSEN telefonisch(!) oder über einen anderen, vom betroffenen System unabhängigen Kanal, informiert werden. Dabei folgende Informationen bereithalten:
   4.1. Um welches Gerät handelt es sich, wo befindet es sich und wie ist bzw. war es aktuell ins Firmennetzwerk eingebunden?
   4.2. Wodurch ist der Virus bemerkt worden (ggf. welcher Virenscanner, Meldungen / Bemerkungen in Dokumenten, Abstürze, Fehlermeldungen, ...)?
   4.3. Bei Meldung durch Virenscanner: Welcher Virus ist gefunden worden?
   4.4. Wodurch kann es zu einer Virus-Verseuchung gekommen sein (E-Mail, Webseite, Download, Netzwerk, USB-Stick, CD, ...)?
   4.5. Könnte es sein, dass der Virus an andere weitergegeben wurde (E-Mail, USB-Stick, Netzwerk, USB-Stick, CD, ...)?
   4.6. Auf weitere Anweisungen des IT-Administrators warten!
5. Falls man eine Internetverbindung hat, kann man nach Rücksprache und auf Anweisung der IT-Administratoren ggf. den Computer über einen online verfügbaren Scanner testen lassen:
   5.1. https://www.trendmicro.com/de_de/forHome/products/housecall.html/
   5.2. https://www.eset.com/de/home/online-scanner/
   Dabei sollte eine Log-Datei, falls verfügbar, gespeichert und an die zentrale IT-Administration in Aachen geleitet werden, um ggf. andere gefährdete Systeme zu identifizieren und die Infektionen schneller beseitigen zu können.
6. Zur weiteren Beweissicherung und ggfs. weiterer forensischer Untersuchung durch externe Spezialisten den Rechner umgehend nach Anweisung an die IT-Administration übergeben.

14 Meldungen von Sicherheitsereignissen und -vorfällen

[INFO] Auch bei bestem Bemühen kann es vorkommen, dass durch ungünstige Umstände Sicherheitsmaßnahmen nicht oder nicht ausreichend eingehalten werden oder dass durchgeführte Maßnahmen nicht

ausreichend wirksam sind („Sicherheitsereignisse“). Ein einzelnes Sicherheitsereignis oder eine Verkettung von Sicherheitsereignissen können zu einem „Sicherheitsvorfall“ führen, bei dem eine erhebliche Wahrscheinlichkeit besteht, dass Information, IT-Systeme oder Prozesse kompromittiert werden und die Informationssicherheit oder der Datenschutz bedroht wird.
Jeder einzelne Mitarbeiter MUSS Beobachtungen oder Entdeckungen, die möglicherweise oder tatsächlich mit Sicherheitsereignissen und -vorfällen im Zusammenhang stehen, ohne Verzögerung den zuständigen Mitarbeitern melden. Dies sind

- der CISO bzw. Datenschutzbeauftragte oder der BCMO als Vertreter des CISO,
- der Leiter IT,
- die IT-Administratoren (bei Sicherheitsereignissen / -vorfällen im Zusammenhang mit IT-Systemen),
- je nach Sachlage außerdem Teamleiter, Systemverantwortliche, Standortleiter, Leiter der Business Unit und der KISTERS Vorstand.

Zur Meldung allgemeiner Sicherheitsereignisse SOLL soweit möglich der Jira Service Desk Informationssicherheit, zur Meldung IT-spezifischer Sicherheitsereignisse der Jira Service Desk System-Administration genutzt werden.
Sofern Kunden oder Partner von den Sicherheitsereignissen oder –vorfällen betroffen sind, so werden diese vom CISO/Datenschutzbeauftragten oder einem autorisierten Vertreter schnellstmöglich benachrichtigt.
Wenn möglich SOLLEN außerdem Maßnahmen zur Behebung bzw. Eindämmung von möglichen Schäden eingeleitet werden:

- Selbstständige persönliche Behebung von Missständen, z.B.
  - Schließen von offenen Zugängen (Fenster, Türen, usw.),
  - Sichern von Information (z.B. Ausdrucken an Druckern, Flipcharts o.ä.),
  - Sperren/Herunterfahren von ungenutzten/ungeschützten IT-Systemen sofern möglich;
- Ansprechen von Kollegen auf potentielle Fehler durch Unaufmerksamkeit oder Unwissenheit,
- Benachrichtigung des/der Vorgesetzten und des Verantwortlichen für die betroffene Information bzw. das betroffene System soweit bekannt.

Die Durchführung dieser Maßnahmen SOLLEN dabei keine Spuren verwischen oder zerstören, die beim Verdacht auf einen Straftatbestand zur weiteren Aufklärung und Ermittlung der Verursacher dienen können.

14.1 Whistle Blowing

Falls ein Mitarbeiter ein Sicherheitsereignis melden möchte, das im Zusammenhang mit einem vermuteten oder tatsächlichen Verstoß gegen nationale und internationale Gesetze, Vorschriften oder ethische Standards steht, SOLL dieses Ereignis gemäß der KISTERS Whistleblowing-Leitlinie an die interne Meldestelle gemeldet werden. Das Whistleblowing-Team MUSS unter Wahrung der Vertraulichkeit der meldenden Person diese Meldung weiterverfolgen und die jeweils zuständigen Verantwortlichen informieren, um mögliche Schäden zu verhindern oder mindestens einzudämmen.
Zur Meldung SOLL soweit möglich der Jira Service Desk Whistleblowing genutzt werden.

15 Disziplinarische Maßnahmen

Falls bei der Analyse eines Sicherheitsereignisses oder -vorfalls durch den CISO, BCMO oder Head IT der Verdacht entsteht, dass die Ursache im schuldhaften Verhalten eines Mitarbeiters liegt, z.B. durch potenzielle Verletzungen von Gesetzen, Regeln, Vorschriften oder internen Richtlinien, MUSS der Verantwortliche den Fall weiter untersuchen.
Wenn der Verdacht bestätigt wird, MUSS der Verantwortliche weitere Maßnahmen ergreifen:

- Bei leicht fahrlässigem Verhalten mit geringem Schaden MUSS der Mitarbeiter über die relevanten Richtlinien belehrt werden. Dies KANN direkt durch den CISO, einen Vertreter oder durch den unmittelbaren Vorgesetzten des Mitarbeiters geschehen.
- Bei leicht fahrlässigem Verhalten mit hohem Schaden MÜSSEN der unmittelbare Vorgesetzte und die Leitung der betroffenen Business Unit informiert werden. Diese KANN eine Ermahnung aussprechen und die Aussetzung oder Aufhebung von bestehenden Zugangs- und Zugriffsrechten veranlassen. Weiterhin KANN die Leitung der Business Unit den KISTERS Vorstand informieren.
- Bei grob fahrlässigen oder vorsätzlichen Handlungen, die die Sicherheit von Daten, Informationen, Anwendungen oder IT-Systemen gefährden, MUSS zusätzlich immer der KISTERS Vorstand informiert werden. Solche Handlungen sind beispielsweise:
    - Missbrauch von Daten, der finanziellen Verlust verursachen kann,
    - unberechtigte Zugriff auf Informationen oder ihre Änderung und unbefugte Übermittlung,
    - illegale Nutzung von Informationen der KISTERS Gruppe,
    - Gefährdung der Informationssicherheit der KISTERS Gruppe oder Geschäftspartnern,
    - Gefährdung des Datenschutzes für Mitarbeiter oder Geschäftspartner,
    - Schädigung des Rufes der KISTERS Gruppe oder Geschäftspartnern.

  Der KISTERS Vorstand KANN weitere disziplinarische und arbeitsrechtliche Maßnahmen wie Abmahnung oder Kündigung aus besonderem Grund aussprechen.
  Unabhängig von den disziplinarischen Maßnahmen KÖNNEN weitere Schritte eingeleitet werden, wie z.B. zivil- und strafrechtlichen Verfahren, in denen auch Haftungsansprüche und Regressforderungen erhoben werden können.

16 Mitgeltende Dokumente

- KISTERS Klassifikation der Informationswerte - Zutritts-, Zugangs- und Zugriffskontrolle (Bestandteil dieser Richtlinie)
- KISTERS Passwortrichtlinie (Bestandteil dieser Richtlinie)
- KISTERS IS Richtlinie für Administratoren (Erweiterung dieser Richtlinie für alle Mitarbeiter mit administrativen Rechten auf KISTERS IT-Systemen)
- KISTERS IS Richtlinie für den Umgang mit externen Dritten (Erweiterung dieser Richtlinie für alle Mitarbeiter, die Ansprechpartner für Kunden, Partner, Lieferanten und Dienstleister sind)
- KISTERS IS Leit- und -Richtlinie zu kryptographischen Maßnahmen (Erweiterung dieser Richtlinie)
- KISTERS Corporate Policy on the Use of Artificial Intelligence Tools
- KISTERS Whistleblowing Leitlinie

17 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*in	Aktion
5.6	2025-07-10	J. Rade	Ergänzungen im Bereich Datenschutz, Ergänzung Regelungen zu Sprachassistenten, Sichtschutzfolien und KI-Assistenzsystemen, Ergänzung BCM im Bereich Einhaltung zur Verpflichtung (in Projekten)
5.5	2024-10-18	J. Rade	Ergänzung Postfach „mailsecurity@kisters.de“ als Kontaktadresse zur Weiterleitung und Bearbeitung von (potentiell) bösartigen E-Mails.
5.4	2024-09-05	H.-J. Schlebusch	Freigabe Gesichtserkennung für Entsperren von Smart-Phones, Ergänzungen: zeitliche Befristung von Ausnahmen, genehmigungspflichtige Internetdienste, mitgeltende Dokumente
5.3	2024-07-18	H.-J. Schlebusch	Ergänzungen: Installation von Software (Freigabe); Korrektur: Verhalten bei Verdacht auf Schadsoftware
5.2	2023-11-14	H.-J. Schlebusch	Behandlung von Abweichungen und Ausnahmen; verschiedene kleine Korrekturen und Ergänzungen
5.1	2023-09-08	H.-J. Schlebusch	Erweiterung "Kontaktpersonen"; Änderung der "zulässige Nutzung"; Anpassung von "Whistleblowing" an die "Whistleblowing Policy"
5.0	2022-09-19	H.-J. Schlebusch	Nutzung von Aufzeichnungsgeräten ergänzt, Nutzung außerhalb KISTERS Betriebsstätten konkretisiert, Anpassungen aufgrund Nutzung von Cloud-Diensten, verschiedene redaktionelle Änderungen
4.4	2021-08-24	H.-J. Schlebusch	Information zu Verschlüsselung mobiler Datenträger
4.3	2021-03-12	H.-J. Schlebusch	Überprüfung, kleinere redaktionelle Korrekturen
4.2	2020-11-11	H.-J. Schlebusch	Anpassungen zur Umstellung der E-Mail von IBM Notes auf Outlook
4.1	2020-08-04	H.-J. Schlebusch	Ergänzung zu E-Mail Nutzung, HomeOffices; Transport und Verwendung außerhalb von KISTERS Betriebsstätten
4.0	2020-04-17	H.-J. Schlebusch	Neue Kapitel: Software-Installation, private Geräte; Erweiterungen: zusätzliche Richtlinien für Telearbeitsplätze, "Vertraulichkeit" von Geschäftsdaten Dritter
3.9	2020-01-14	H.-J. Schlebusch	Ergänzungen zu Entsperrung von Smartphones
3.8	2019-07-15	H.-J. Schlebusch	Nutzung außerhalb KISTERS Betriebsstätten; Nutzung von internet-basierten Diensten in Kooperationen
3.7	2019-03-08	H.-J. Schlebusch	Neuer Abschnitt „Disziplinarische Maßnahmen“, kleinere Fehlerkorrekturen
3.6	2018-08-08	H.-J. Schlebusch	Datenschutzthemen, Backup vs. Archivierung, redaktionelle Änderungen
3.5	2017-11-15	H.-J. Schlebusch	Konkretisierung “Clean desk - clear screen”
3.4	2017-07-20	H.-J. Schlebusch	Beweissicherung

Version	Datum	Editor*in	Aktion
3.3	2017-07-09	H.-J. Schlebusch	Disziplinarische Maßnahmen, Bluetooth/NFC für Mobilgeräte
3.2	2017-04-19	H.-J. Schlebusch	„KISTERS Informationssicherheitsrichtlinie für Administratoren“ als separates Dokument
3.1	2017-01-30	H.-J. Schlebusch	Kleinere Ergänzungen und Modifikationen nach Review Chr. Aust
3.0	2016-11-10	Bernd Kisters, H.-J. Schlebusch	Reorganisation; separate Dokumente für „KISTERS Passwortrichtlinie“ „KISTERS Zutritts-, Zugangs- und Zugriffskontrolle“
2.3	2016-10-05	Bernd Kisters, H.-J. Schlebusch	Verschiedene Ergänzungen, IT-Sicherheit -> Informationssicherheit, Schlüsselworte nach RFC2119
2.2	2016-06-08	Bernd Kisters	Überarbeitung/Ergänzungen
2.2	2016-07-04	H.-J. Schlebusch	Veröffentlichung Confluence
2.1	2016-06-03	H.-J. Schlebusch	Geltungsbereich, Ergänzungen für Kommunikationstools
2.0	2015-10-09	H.-J. Schlebusch	Überarbeitung für ISO 27001
1.0	2013-08-09	Bernd Kisters	Erstellung