DS/

Gemeinsam besser

Information Technology (IT-) Governance

Diersch & Schröder Unternehmensgruppe
Stand 2024

ENERGIE

CHEMIE

YOUNG BUSINESS

DS / WESER-PETROL

DS / MINERALÖL

DS / CARD+DRIVE

CARD+DRIVE Polska

LANFER ENERGIE

EMOVA
Energie. So einfach.

LANDS

UTG
Unabhängige Tanklogistik GmbH

ENERGU

HAUER
Energie mit Sympathie

WESER TANKING

LEU.

ADDITIV CHEMIE LUERS

ESTICHEM AS

ACF

LEVACO CHEMICALS

Sparks

SCS

ELAPRO

ecopox

polytives

Lynatox

DS / DIERSCH & SCHRÖDER

INHALT

SEITE	KAPITEL
05	Ziele der IT-Governance
06	Verantwortung
08	Nutzung von IT-Systemen
11	Protokollierung
11	Missbrauchskontrolle
12	(Vermutete) Attacken durch Viren, Hacker und ähnliches
13	Umgang mit sozialen Medien
14	Beschaffung / Einkauf (Hard und Software)
14	Cyber-Versicherung
14	Umgang mit Künstlicher Intelligenz
14	Verstoß gegen die IT-Governance

VORWORT

Liebe Leserinnen und Leser,

die rasante Entwicklung in unserer digitalisierten Welt bringt nicht nur Chancen, sondern auch neue Herausforderungen mit sich. Insbesondere die steigende Komplexität und die sich verändernden Angriffsvektoren durch Cyberbedrohungen erfordern ein **hohes Maß an Aufmerksamkeit und Sicherheitsbewusstsein**. Die wachsenden regulatorischen Anforderungen, insbesondere im Rahmen von KRITIS, machen deutlich, dass ein effektiver Schutz unserer digitalen Ressourcen unerlässlich ist.

Mit unserer IT-Governance – die für alle Führungskräfte, Mitarbeiterinnen und Mitarbeiter (nachfolgend gemeinsam „die Beschäftigten“) der Diersch & Schröder GmbH & Co. KG und all ihrer verbundenen Unternehmen (nachfolgend „DS-Gruppe“) verbindlich ist – schaffen wir nicht nur eine **Grundlage für den verantwortungsbewussten Umgang mit unseren IT-Infrastrukturen**, sondern setzen auch ein starkes Zeichen im Hinblick auf die zunehmenden Herausforderungen der **Digitalisierung** unseres Unternehmens.

Gemeinsam tragen wir dazu bei, dass die DS-Gruppe in dieser komplexen und regulierten Umgebung sicher und effizient agieren kann.

Ihre Mitwirkung ist entscheidend, um die digitale Zukunft unserer Organisation zu gestalten und sicherzustellen.

Bremen, den 01. September 2024

Jan Christiansen
Chief Executive Officer
der DS-Unternehmensgruppe

1 Ziele der IT-Governance

Mit dieser IT-Governance möchten wir den Rahmen für effiziente, sichere und geschäftsunterstützende IT-Praktiken setzen. Die genauen Ausführungen, spezifischen Anweisungen und arbeitsvertraglichen Regelungen werden in separaten Dokumenten oder Richtlinien ausführlich behandelt, um den Umfang dieses Dokuments zu reduzieren.

Unsere IT-Governance zielt darauf ab, die Nutzung von Informationstechnologie im Einklang mit den strategischen Zielen der DS-Gruppe zu steuern.

HAUPTZIELE
der IT-Governance

Verständnis
Wir möchten mit der IT-Governance ein gemeinsames Verständnis schaffen, um „GEMEINSAM BESSER" zu werden. *Zum Beispiel durch Schulungen soll das Verständnis gefördert werden.*

Einhaltung von IT-Sicherheitsstandards
Wir möchten uns vor Viren, Trojanern und Schadprogrammen schützen und externe Eingriffe abwehren. *Zum Beispiel durch regelmäßige Aktualisierung von Antivirenprogrammen und Firewalls sowie Sensibilisierung der Beschäftigten für sichere Online-Praktiken.*

Schutz unternehmenskritischer und personenbezogener Daten
Wir möchten die Sicherstellung der Vertraulichkeit und Integrität sensibler Informationen garantieren. *Zum Beispiel durch Implementierung von Verschlüsselungsmaßnahmen für personenbezogene Daten und Einführung strenger Zugriffssteuerungsrichtlinien.*

Sicherer und nachhaltiger Betrieb der IT-Infrastruktur
Wir möchten einen stabilen, sicheren und nachhalten Betrieb für reibungslose Geschäftsprozesse sicherstellen. *Zum Beispiel durch regelmäßige Wartung der IT-Systeme, um deren Leistungsfähigkeit sicherzustellen, sowie Implementierung von Notfallplänen zur schnellen Wiederherstellung im Falle von Ausfällen.*

Gesetzeskonformer Umgang mit der IT-Infrastruktur
Wir möchten – insbesondere im Kontext kritischer Infrastrukturen – relevante, gesetzlichen Vorschriften erfüllen. *Zum Beispiel durch Implementierung von Maßnahmen zur Einhaltung von Datenschutzbestimmungen, branchenspezifischen Regularien und weiteren relevanten Gesetzen.*

Eine grundlegende Voraussetzung ist dabei die Kooperation an der Verwirklichung dieser Ziele mitzuwirken, die sich über alle Geschäftseinheiten und Beschäftigten der DS-Gruppe erstreckt.

2 Verantwortung

2.1 Rolle der Muttergesellschaft und des ISB

Die Geschäftsführung der Diersch & Schröder GmbH & Co. KG und der Informationssicherheitsbeauftragte (ISB) sind maßgeblich für den Inhalt und die Überwachung der IT-Governance verantwortlich. Der ISB leitet, überwacht und verbessert kontinuierlich die Informationssicherheit in der DS-Gruppe. Bei Informationssicherheitsvorfällen ist der ISB einzubeziehen.

Die Diersch & Schröder GmbH & Co. KG gewährleistet, dass Beschäftigte die erforderlichen Schulungen, Instruktionen und Anweisungen für den Umgang mit IT-Systemen, Medien und Daten erhalten.

2.2 Geschäftsführungen der Tochtergesellschaften

Die jeweilige Geschäftsführung des Unternehmens der DS-Gruppe (nachfolgend auch „DS-Einheit") ist verantwortlich für die Umsetzung der IT-Governance und deren Kommunikation an die Mitarbeiterinnen und Mitarbeiter. Die IT-Verantwortlichen gewährleisten den Betrieb der IT-Infrastruktur und IT-Systeme.
Der ISB unterstützt sie dabei.

2.3 Beschäftigte

Jeder Beschäftigte der DS-Gruppe hat die Regelungen der IT-Governance einzuhalten, trägt aktiv zur Sicherheit unserer IT-Infrastruktur bei und handelt verantwortungsbewusst im Umgang mit Daten, Endgeräten und IT-Systemen.

3 Nutzung von IT-Systemen

Die IT-Systeme und Infrastrukturen, die wir als DS-Gruppe bereitstellen, sind wichtige Werkzeuge für die tägliche Arbeit. Die darin enthaltenen Daten sind integraler Bestandteil dieser Systeme. Sowohl die IT-Systeme als auch ihre Daten bleiben während der gesamten Nutzungsdauer Eigentum der DS-Gruppe.

Wenn die Beschäftigten IT-Systeme nicht mehr nutzen (z. B. wenn sie das Unternehmen verlassen), müssen alle Bestandteile, einschließlich der Daten, an die DS-Gruppe zurückgegeben werden.

Um sicherzustellen, dass die Systeme einwandfrei funktionieren, werden sie regelmäßig überprüft und gewartet. Die DS-Gruppe setzt dafür auch externe Dienstleister ein. Die Beschäftigten sind dazu aufgefordert, die Arbeit dieser Experten zu unterstützen und sicherzustellen, dass alles reibungslos läuft. Geplante Wartungen werden rechtzeitig angekündigt.

3.1 Private IT-Systeme

3.1.1 Nutzung im Unternehmensnetzwerk (LAN, WLAN)

Die Nutzung von privaten IT-Systemen, wie Desktops, Notebooks oder sonstigen Systemen oder IT-Komponenten, innerhalb des Unternehmensnetzwerkes (z. B. durch das Anschließen an einen Netzwerkanschluss oder Einbinden in das WLAN) der DS-Gruppe, ist nicht erlaubt.

3.1.2 Zugriff auf Daten, Applikationen und Services des Unternehmens (-Netzwerkes)

Der Zugriff auf Daten und Services des Unternehmensnetzwerkes (z. B. MS365 Applikationen, Citrix, VPN) auf privaten Geräten ist ausschließlich für private Mobiltelefone und Tablets (z. B. IPad), die im Rahmen des BYODS (Bring your own device) Programms (z. B. MS365) genutzt werden können, genehmigt. Diese sind jedoch mittels des eingesetzten mobilem Gerätemanagement (z. B. Intune) abzusichern.

3.2 Private Nutzung von IT-Systemen

Grundsätzlich ist eine private Nutzung von IT-Systemen nicht gestattet. Ausnahmen der Nutzung von dienstlichen Telefonen und Mobilgeräten sind in der „Richtlinie für Kommunikationsmedien" und ggf. in arbeitsvertraglichen Regelungen vorgesehen.

Für die Nutzung des Firmenhandys gilt, dass außerhalb der Arbeitszeit die private Nutzung des Handys (Internet, Telefon, Apps etc.) nach wie vor erlaubt ist. Es ist nicht gestattet, die Firmen-Kontaktdaten (E-Mail-Adresse, Telefonnummer und jegliche Äquivalente) für private Zwecke zu nutzen.

3.3 Umgang mit dienstlichen E-Mails

Bei der Nutzung des dienstlichen E-Mail-Accounts sind folgende Punkte zu beachten:

Anhänge
Vermeidung von Anhängen – stattdessen sollten Dateien an einem gemeinsamen Speicherort geteilt werden (z. B. OneDrive).

Externe E-Mails
Externe E-Mails werden als solche gekennzeichnet. Trotz aller Sicherheitsmaßnahmen gilt eine besondere Vorsicht beim Öffnen von Anhängen und Links.

Adressatenkreis „Need to Know"
Reduzierung von „cc/Kopie" auf ein notwendiges Maß. Hinterfragung, ob alle Adressaten diese Information benötigen oder erhalten dürfen.

Abwesenheit
Bei Abwesenheiten ab einem Arbeitstag ist eine automatische Antwort an die Sender mit voraussichtlichem Antwortdatum einzurichten.

Chat vs. E-Mail
Vermeidung von ‚Ping-Pong' E-Mails als Frage-Antwort-Verlauf. Hierfür ist die Chat Funktion von M.S. Teams oftmals effektiver.

Weiterleitung
Eine automatische Weiterleitung an E-Mail-Adressen außerhalb der DS-Gruppe ist untersagt. Das gilt auch für die Weiterleitung an private E-Mail-Adressen des Benutzers.

Signatur
Die automatische Fußzeilen in E-Mails (Signaturen), die rechtliche Ausschlusserklärungen enthalten, dürfen weder gekürzt, ergänzt noch gänzlich entfernt werden.

3.4 Passwörter

Der Schutz von Passwörtern liegt in der Verantwortung der Beschäftigten. Hierbei gilt zu beachten:

- **Geheimhaltung:** Passwörter müssen geheim gehalten werden und dürfen nicht weitergegeben werden.
- **Keine unsicheren Aufzeichnungen:** Das Aufschreiben auf Papier oder unverschlüsseltes Speichern auf Systemen oder Medien ist zu vermeiden.
- **Verdacht der Kompromittierung:** Bei Kompromittierung oder dem Verdacht der Kompromittierung sollten Passwörter sofort geändert werden.

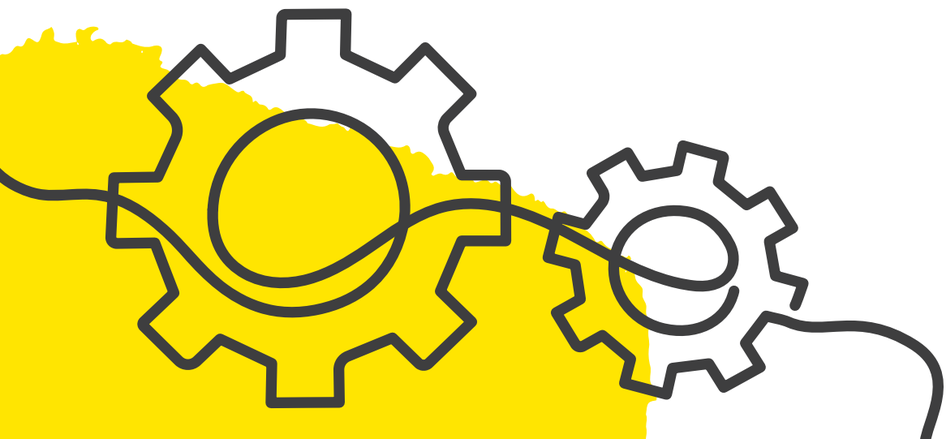
- **Starke Kennwörter:** Verwendung von starken Kennwörtern. Falls das IT-System keine speziellen Vorgaben macht, sollen Passwörter optimalerweise Großbuchstaben, Kleinbuchstaben, Ziffern/Zahlen und Sonderzeichen enthalten. Die Länge des Passwortes darf 8 Zeichen nicht unterschreiten, empfohlen sind mehr als 10 Zeichen.
- **Passphrase:** Nutzung einer sog. Passphrase, damit ein komplexes Passwort erstellt werden kann, dass aber merkbar bleibt.
- **Unterschiedliche Kennwörter:** Nutzung von unterschiedlichen Passwörtern für geschäftliche und private Zwecke.

Alle Systeme müssen passwortgeschützt sein. Single Sign-On, wie die Authentifizierung durch einmalige Systemanmeldung ist zu bevorzugen.

3.5 Softwarenutzung und/oder Installation

Die Einführung von Software erfolgt nach Bedarf und kann ggf. einen Projektinitiierungsprozess notwendig machen. Test- und Demoversionen bedürfen vorheriger Absprache und Freigabe durch die IT-Abteilung.

- **Datenschutzfreigabe:** Es ist zwingend erforderlich, dass jede eingesetzte Software in das Verfahrens- und Softwareverzeichnis aufgenommen und bei datenschutzrechtlicher Relevanz vom Datenschutzbeauftragten (DSB) freigegeben wird.
- **Informationssicherheit:** Die Nutzung von Anwendungen gleich welcher Art (SaaS, Web-Applikationen, Portale, Apps, stationär installierte Anwendungen etc.) ist in Abstimmung mit der IT zu erfolgen die eventuelle Freigabe (z. B. ISB, DSB) einfordert.
- **Lizenzen:** Privat lizenzierte oder unlizenzierte Software (Raubkopien) sind strikt verboten. Ebenso untersagt ist der Download und die Speicherung von Programmen sowie Dateien für nicht berufliche Zwecke auf IT-Systemen der DS-Gruppe.
- **Sicherheitsmaßnahmen:** Software und Daten, die gegen die Regeln verstoßen oder als betriebs- oder sicherheitskritisch eingestuft werden, können ohne Vorankündigung gelöscht werden, ggf. automatisch durch technische Sicherheitsmaßnahmen.



- **Dateiablage:** Die Ablage von Dateien auf Arbeitsplatzsystemen oder Mobilgeräten erfolgt ausschließlich unter Nutzung von Synchronisation mit freigegebenen Cloud-Anbietern (z. B., Microsoft OneDrive), was stetige Aktualisierung und Sicherheit gewährleistet. Lokale nicht synchronisierte Dateiablagen sind untersagt.
- **Softwareinstallation:** Die Installation von Software wird durch die IT-Abteilung durchgeführt. Eine eigenständige Installation von Software ist untersagt.

Diese Regelungen gelten identisch für stationär installierte oder auch sog. SaaS (z. B. Cloud / Internetportale) Anwendungen.

3.6 Notebooks, Tablets und Smartphones, Mobile IT-Systeme

3.6.1 Nutzung von mobilen IT-Systemen

Mobile IT-Systeme wie Notebooks, Tablets, Smartphones usw. sind Risikofaktoren für den unbefugten Zugriff auf DS-Gruppeninformationen. Beschäftigte dürfen ihre mobilen Geräte nicht an Dritte weitergeben.

Bei externer Nutzung muss sichergestellt werden, dass sensible Informationen nicht in falsche Hände gelangen. Es wird empfohlen, besonders schutzbedürftige Daten an Orten zu verarbeiten, die nicht von Dritten einsehbar sind.

Die Speicherung von Daten auf mobilen Geräten sollte nur für die Aufgabenerfüllung der Beschäftigten erfolgen, da der lokale Speicher keiner Datensicherung unterliegt. Grundsätzlich ist darauf zu Achten, dass sämtliche Informationen ausschließlich auf freigegebenen Speicherorten abgelegt werden. Verschlüsselung ist technisch zu gewährleisten und die Daten müssen den Synchronisationsanforderungen entsprechen.

3.6.2 Zentrale Verwaltung

Die Verwaltung der mobilen IT-Systeme, einschließlich Software-Installation, erfolgt über das zentrale Mobile Device Management (MDM). Alle mobilen Endgeräte müssen mit MDM verbunden sein, und die Nutzung ohne Anschluss an dieses System ist nicht gestattet.

3.6.3 Diebstahl und Verlust

Verlorene oder gestohlene IT-Systeme müssen umgehend der IT-Abteilung gemeldet werden. Diese informiert den ISB und den DSB. Eine verspätete Meldung kann Bußgelder nach sich ziehen. Bei Diebstahl ist eine Anzeige bei der Polizei erforderlich. Die IT-Abteilung ergreift Schutzmaßnahmen wie z. B. Remote-Sperrung oder Löschung.

3.6.4 Mobile Datenträger

Generell ist die Nutzung von mobilen Datenträgern zu vermeiden, da diese stets ein Sicherheitsrisiko (Verlust, Defekt, Kompromittierung) darstellen. Es müssen Vorkehrungen getroffen werden, um den Verlust von Datenträgern gespeicherten Informationen zu unterbinden. Hierbei sind die Vorgaben der IT-Abteilung zu beachten. Nicht mehr verwendete Datenträger müssen durch die IT-Abteilung entsorgt werden.

Sollten Beschäftigte einen mobilen Datenträger auffinden, so dürfen solche Datenträger niemals an die IT-Systeme der DS-Gruppe angeschlossen werden. Es ist nicht auszuschließen, dass sich auf dem Datenträger Schad- oder Spionagesoftware befindet.

Gefundene Datenträger sind der IT-Abteilung zu melden und werden sorgfältig von dieser im Hinblick auf schädliche Inhalte inspiziert und vernichtet.

3.7 Nutzung externer Plattformen (z. B. Cloud-Dienste)

Externe Plattformen, erreichbar über das Internet, dürfen nur betriebsnotwendig und in minimaler Anzahl genutzt werden. Gängige Sicherheitsrichtlinien wie Passwortregeln und 2-Faktor-Authentifizierung sind einzuhalten. Generell sollten Plattformen an das Active Directory angebunden werden, um globale Passwortregeln zu ermöglichen.

- **Begrenzung auf Notwendiges:** Nutzung externer Plattformen ist auf das Betriebsnotwendige zu begrenzen, und die Anzahl ist zu minimieren.
- **Präferenz für bestehende Lösungen/Partner:** Lösungen auf bestehenden Plattformen und Service Providern (z. B. MS365 Umgebung) sind vorzuziehen.
- **Eigentum der Zugangsdaten:** Daten auf externen Plattformen sind Eigentum der DS-Gruppe, unterliegen der IT-Governance, insbesondere im Bereich Passwörter.
- **Sicherheitsstandard prüfen:** Nur Portale, die dem aktuellen Sicherheitsstandard entsprechen, dürfen genutzt werden. Die Überprüfung obliegt der IT-Abteilung der DS-Gruppe.
- **Regelmäßige Sicherheitsüberprüfung:** Nutzer externer Portale sind verpflichtet, regelmäßig und bei Verdacht Rücksprache mit der IT-Abteilung der DS-Gruppe zu halten, um den Sicherheitszustand zu überprüfen.

3.8 Sicherheitsmaßnahmen im Mobilen Office

Für das „Mobile Arbeiten" sind einschlägige Regelungen arbeitsvertraglich getroffen, die bindend sind. Generell ist beim mobilen Arbeiten folgendes zu beachten:

*Auch regelmäßige Prüfung von privaten Netzwerkgeräten zuhause, z. B. Internetrouter auf Firmware Updates.

Bei Fragen zu der IT-Governance wenden Sie sich bitte an die IT-Abteilung der Diersch & Schröder GmbH & Co. KG.
E-Mail: **ITGovernance@ds-bremen.de**

4 Protokollierung

Die Protokollierung von IT-Aktivitäten überwacht nicht nur unsere Systeme, sondern gewährleistet auch die rechtskonforme Gestaltung und Sicherheit unserer IT-Infrastruktur.

Unsere Protokollierung ist darauf ausgerichtet, einen umfassenden Schutz sensibler Daten zu gewährleisten und gleichzeitig höchste Standards in puncto Datenschutz und -sicherheit zu erfüllen.

Die Protokolldaten werden nicht für Leistungs- und Verhaltenskontrollen von Beschäftigten verwendet, sondern ausschließlich zur Erkennung von Störungen, Ausfällen, Sicherheitsvorfällen und Optimierungen.

5 Missbrauchskontrolle

Um den unbefugten Zugriff und unerlaubte Aktivitäten zu verhindern, sind spezielle Maßnahmen zur Missbrauchskontrolle implementiert. Beschäftigte werden dazu aufgefordert, verdächtige Aktivitäten umgehend der IT zu melden.

Im Falle von Missbrauchsverdacht werden folgende Maßnahmen ergriffen:

- **Technische Verhinderung:** Automatische, technische Maßnahmen zur Unterbindung von IT-Infrastruktur-Missbrauch werden in Abstimmung mit dem ISB ergriffen.
- **Personenbezogene Überprüfung:** Eine detaillierte Protokollüberprüfung erfolgt nur bei schwerwiegendem Missbrauchsverdacht, unter zwingender Beteiligung des Compliance Officers.
- **Beteiligung des Compliance Officers:** Der Compliance Officer ist integraler Bestandteil des Überprüfungsprozesses bei erheblichem Missbrauchsverdacht.
- **Löschung bei nicht bestätigtem Verdacht:** Nicht bestätigte Verdachtsmomente führen zur sofortigen Löschung aller überprüften Daten, ohne weitere Folgemaßnahmen.
- **Sofortiges Handeln bei Gefahr im Verzug:** Der ISB ergreift umgehend Maßnahmen zur Unterbindung von gefährdenden Handlungen. In Abstimmung mit dem Compliance Officer sind Strafverfolgungsbehörden einzubeziehen, wenn die Voraussetzungen gegeben sind.

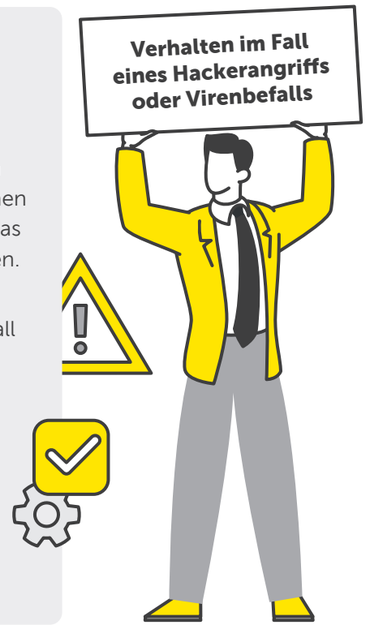
6 (Vermutete) Attacken durch Viren, Hacker und ähnliches

Alle Beschäftigten sind aufgefordert, jegliche Vorfälle oder Sicherheitsverletzungen unverzüglich der IT-Abteilung zu melden. Dabei ist folgendes zu beachten:

6.1 Sofortmaßnahmen

Bei Verdacht auf einen Virenbefall oder Hackerangriff sind schnelle Sofortmaßnahmen entscheidend, um potenzielle Schäden zu minimieren. Durch die Isolierung des betroffenen Systems wird die Ausbreitung von Malware oder Hackeraktivitäten eingedämmt.

- **Netzwerkverbindung trennen:** Umgehende Trennung der Verbindung zu Netzwerken, insbesondere zu Unternehmensnetzwerken oder sensiblen persönlichen Netzwerken. Dies kann durch das Deaktivieren von WLAN oder das Trennen von Netzwerkkabeln erfolgen. Im Zweifel das Gerät vom Stromnetz nehmen / ausschalten.
- **Sicherheitsvorfall melden:** Meldung des Verdachts auf einen Virenbefall oder Hackerangriff unverzüglich der IT-Abteilung. So viele Details wie möglich angeben, um eine schnellere und gezielte Reaktion zu ermöglichen.
- **Sicherheitssoftware aktivieren und scannen:** Umgehenden Systemscan mit installierter Sicherheitssoftware (Antivirenprogramm, Firewall).



6.2 Unverändertes Schadensbild

Das Schadensbild eines Vorfalls darf nicht verändert werden. Diese Maßnahme erleichtert nicht nur die Lösungsarbeit in vielen Fällen, sondern ist auch für eine forensische Aufarbeitung im Schadensfall oft unerlässlich. Im Falle einer Einbeziehung Dritter oder der Entstehung haftbarer Schäden ist die Unverfälschtheit des Schadensbildes sowohl aus Sicht der Strafverfolgung als auch der Versicherung von entscheidender Bedeutung.

Ausnahmen hiervon gelten nur für unmittelbare Verhinderungs- und Vereitelungsmaßnahmen, die sofort ergriffen werden können.

6.3 Kein direkter Zugriff auf infiltrierte Systeme

Im Falle infiltrierter Systeme, wie beispielsweise Hacker-Angriffe, darf kein direkter Zugriff auf das infiltrierte System erfolgen, auch nicht durch Administratoren. Dies dient dem Schutz der Integrität der Daten und der Sicherstellung einer umfassenden Analyse des Vorfalls durch die IT-Sicherheitsexperten.

7 Umgang mit sozialen Medien

Die Nutzung von sozialen Medien im beruflichen Kontext erfordert Achtsamkeit, um potenzielle Sicherheitsrisiken zu minimieren. Beschäftigte sind angehalten, die folgenden Vorgaben strikt zu befolgen.

- **Vermischung beruflicher und privater Sphäre:** Soziale Netzwerke wie Facebook, Instagram, LinkedIn, XING und X (ehemals Twitter) sind ausschließlich für private Zwecke zu nutzen. Eine dienstliche Nutzung erfolgt ausschließlich in Zusammenarbeit mit der Marketing-Abteilung.
- **Verantwortungsbewusste Online-Präsenz:** Alle Online-Aktivitäten sind nicht anonym und können von der Öffentlichkeit, einschließlich Kollegen, Kunden, Lieferanten und Wettbewerbern, eingesehen werden.
- **Schutz von Unternehmensinformationen:** Betriebliche Interna oder Betriebsgeheimnisse, Informationen zur Unternehmensstrategie und zur wirtschaftlichen Situation der DS-Gruppe dürfen nicht öffentlich geteilt werden. Personenbezogene Daten dürfen nicht ohne Zustimmung des Betroffenen geteilt werden.
- **Beachtung von Urheberrechten:** Urheberrechte und Copyrights bei Musik, Filmen, Bildern und Unternehmenslogos müssen beachtet werden, genauso wie das Recht am eigenen Bild.
- **Klarstellung persönlicher Meinungen:** Bei persönlichen Meinungsäußerungen, auch im Kontext des Unternehmens, ist es wichtig zu betonen, dass es sich um persönliche Ansichten handelt. Fakten sollten korrekt sein, und Beschäftigte sollten sich bewusst sein, dass sie möglicherweise als Repräsentanten des Unternehmens gelten, auch ohne explizite Angabe.
- **Dauerhafte Konsequenzen von Beiträgen:** Angaben und Beiträge im Internet sind oftmals dauerhaft sichtbar. Selbst wenn ein Beitrag gelöscht wird, kann eine dauerhafte Speicherung nicht verhindert werden.
- **Verwaltung von Unternehmensprofilen:** Mitarbeiterinnen und Mitarbeiter, die Unternehmensseiten der DS-Gruppe in den sozialen Medien betreuen, sind dazu verpflichtet, die Zugänge mittels Zwei-Faktor-Authentifizierung (2FA) vor unberechtigtem Zugriff zu schützen. Nach Austritt aus der DS-Gruppe sind sie aus den Unternehmensseiten zu entfernen.

8 Beschaffung / Einkauf (Hard und Software)

Verantwortlich für die Beschaffung jeglicher Hard- und Software ist die IT-Abteilung. Alle Beschaffungen von Hardware und Software müssen den festgelegten Richtlinien und Prozessen entsprechen. Dies gewährleistet, dass die erworbenen Ressourcen sicher und kompatibel sind. Für die Beschaffung existiert ein einheitlicher Hardwarekatalog, der definiert welche Hardware für Endanwender (z. B. Notebooks, PCs, Drucker, Monitore etc.) zum Einsatz kommt.

9 Cyber-Versicherung

Jede DS-Einheit muss sich gegen Cyber-Vorfälle absichern. Die Verantwortung für die Sicherstellung der Versicherung obliegt der Geschäftsführung der jeweiligen DS-Einheit in Abstimmung mit der Versicherungsabteilung der Diersch & Schröder GmbH & Co. KG.

10 Umgang mit KI

- **Menschliche Handlungsmacht:** Verwendete KI-Systeme müssen so gestaltet sein, dass die Beschäftigten die Entscheidungsgewalt über wichtige Angelegenheiten behalten. Automatisierte Entscheidungen müssen überwacht und bestätigt werden können.
- **Datenschutz:** KI-Anwendungen müssen sicherstellen, dass personenbezogene Daten geschützt und gemäß den Datenschutzbestimmungen verwaltet werden, um die Privatsphäre der Beschäftigten, Kunden und Dienstleister zu wahren. Sensible Daten sollten möglichst anonymisiert und pseudonymisiert werden, sodass sie nicht mehr direkt bestimmten Personen zugeordnet werden können.
- **Einführung neuer KI-Systeme:** Bei der Einführung neuer KI-Systeme müssen folgende Stakeholder involviert werden: Compliance Officer, ggf. DSB, ISB, IT-Abteilung und Risikomanagement.

11 Verstoß gegen die IT-Governance

Die Einhaltung dieser IT-Governance wird stichprobenartig überprüft. Ein Verstoß gegen diese IT-Governance wird, wenn er festgestellt wird, an die Geschäftsführung der jeweiligen DS-Einheit, an den ISB sowie, den Compliance Officer und die Personalabteilung gemeldet. Der Verstoß kann zu arbeitsrechtlichen Konsequenzen führen.

DS/

Gemeinsam besser

ENERGIE

Gemeinsam besser für **Mobilität**,
Wärme und **Strom** – das treibt uns an.

CHEMIE

Unsere **Additive** schmieren industrielle
Produktionsanlagen und schützen Bananenpflanzen.

YOUNG BUSINESS

Start-ups helfen der DS-Gruppe, **jung** und **innovativ** zu bleiben.