Konzernsicherheitsrichtlinie

1. Geltungsbereich

Die vorliegende Konzernsicherheitsrichtlinie ist räumlich-personell für alle Mitarbeiter der Maschinenfabrik Reinhausen GmbH (MR) sowie der konzernzugehörigen Unternehmen verbindlich (Reinhausen Konzern); die Übertragung auf die einzelnen Tochtergesellschaften erfolgt durch konkrete Beschlussfassung und Bekanntmachung der jeweiligen Geschäftsführung, erforderlichenfalls unter Berücksichtigung landesspezifischer Vorschriften.

Mitarbeiter des Reinhausen Konzern, welche einem Konzerndritten physischen Zugang zu dem Betriebsgelände oder Zugriff auf IT-Systeme erteilen, haben sicherzustellen, dass die relevanten Regelungen der Konzernsicherheitsrichtlinie mit ihren Anlagen auch durch die jeweiligen Konzerndritten eingehalten werden.

Diese Konzernsicherheitsrichtlinie regelt die Informationssicherheit von IT- und OT-Systemen, betrifft also Prozesse sowie den physischen Schutz des Betriebsgeländes im Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität. Explizit nicht erfasst sind Aspekte der Arbeitssicherheit von Mitarbeitern (m/w/d). Als Teil des integrierten (Risiko-) Management-Systems (IMS) ist die Konzernsicherheitsrichtlinie um den Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken bemüht. Diese Konzernsicherheitsrichtlinie (V3) ersetzt mit Wirkung zum 14.07.2023 die Version V2.

2. Sicherheitsmanagement

2.1 Organisation und Verantwortung

Die Geschäftsführung der MR verantwortet die Sicherheit von Informationen und Daten des Unternehmens; dies umfasst Verfügbarkeit, Vertraulichkeit und Integrität. Zur Wahrnehmung/Koordination dieser Aufgabe wird diese an einen Konzernsicherheitsbeauftragten (Security Officer) delegiert, welcher an die verantwortliche Geschäftsführung der MR berichtet. Das nachfolgend dargestellte Konzernsicherheitsteam berichtet an den Security Officer und besteht aus den folgenden Fachbereichen mit den dargestellten Kompetenzen:

- IT-Sicherheit & Systemtechnik (Technology): Sicherheit der Informationstechnologie,
- Informationssicherheit Produkte & Datenschutz (Information): Datenschutzkoordinator, Kommunikation mit dem externen Datenschutzbeauftragten;
- Werkssicherheit physisch außen & innen (Location): physische Sicherheit der Standorte.

Die Organisation des Sicherheitsmanagements im Sinne des IMS sowie die zuständigen Ansprechpartner finden Sie im GroupNet unter KONZERN, Konzernsicherheit & ESG und in der Delegationsmatrix des Reinhausen Konzern.

Zudem verantwortet die Geschäftsführung der MR die Managementsysteme und bildet gemeinsam mit dem Sustainability Officer und dem Compliance Officer das ESG-Team (Environmental Social Governance). Der Security Officer, der Sustainability Officer und der Compliance Officer werden sich regelmäßig sowie anlassbezogen informieren und geeignet einbinden.

Soweit beschriebene Methoden aus technischen bzw. gesetzlichen Gründen an einem Standort nicht umsetzbar sind, bedürfen Abweichungen der Zustimmung des Konzernsicherheitsbeauftragten. Die Beteiligungsrechte des zuständigen Betriebsrates bleiben gewahrt. Informationen zur Konzernsicherheit sowie den Verantwortlichen finden sich im GroupNet.

2.2 Rechte und Pflichten

Jede Nichteinhaltung dieser Konzernsicherheitsrichtlinie kann ein unternehmensweites Risiko auslösen. Verstöße gegen diese Konzernsicherheitsrichtlinie, potenzielle Gefährdungen sowie der Verlust oder die Korruption von Informationen und Geräten müssen umgehend den im GroupNet dokumentierten Stellen gemeldet werden.

Jeder Lieferant und Dienstleister muss vor Aufnahme seiner Tätigkeit die Erklärung zur Verschwiegenheitspflicht (Non Disclosure Agreement/NDA) unterschreiben, sofern er Zugriff auf vertrauliche Daten oder Informationen haben kann; verantwortlich für die Beurteilung ist der jeweilige Auftraggeber. Konzerneigene NDA-Formulare werden durch die Rechtsabteilung freigegeben, der auch Vorlagen Dritter zur Prüfung vorzulegen sind; auf dieser Basis werden NDAs mit Lieferanten und/oder Dienstleistern durch den Fachbereich gezeichnet.

Bei Zugriff von Dritten auf personenbezogene Daten werden – erforderlichenfalls unter Einbindung des Datenschutzbeauftragten – Auftragsdatenverarbeitungsverträge gemäß DSGVO abgeschlossen. Jedes tatsächliche oder vermeintliche sicherheitsrelevante Ereignis muss vertraulich behandelt werden; alle Anfragen zu diesbezüglichen Ereignissen müssen zuerst an den Konzernsicherheitsbeauftragten weitergeleitet werden. Verstöße gegen diese Konzernsicherheitsrichtlinie können arbeits-, zivil- oder strafrechtliche Maßnahmen nach sich ziehen – die jeweilige Gesellschaft behält sich das Recht vor, die Einhaltung dieser Konzernsicherheitsrichtlinie zu überprüfen.

3. Nutzung von IT-Systemen

3.1 Rechtliche Grundlagen

Der Reinhausen Konzern stellt den Mitarbeitern zur Erfüllung dienstlicher Aufgaben moderne und dem Stand der Technik entsprechende IT-Systeme zur Verfügung (E-Mail-System, ERP-System, Datenspeicher, Telefonsysteme etc.). Diese IT-Systeme dürfen nur in firmenseitig sowie gesetzlich erlaubter Weise genutzt werden. Es wird ausdrücklich darauf hingewiesen, dass insbesondere folgende Sachverhalte nach dem deutschen Strafgesetzbuch (im Ausland gelten mitunter abweichende Regelungen) unter Strafe gestellt sind (vereinzelt ist schon der Versuch strafbar):

- Ausspähen von Daten (§ 202a StGB);
- unbefugtes Verändern, Löschen, Unterdrücken, Unbrauchbarmachen von Daten (§ 303a StGB);
- Computer-Sabotage (§ 303b StGB) und Computer-Betrug (§ 263a StGB);
- die Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) oder rassistischem Gedankengut (§ 130 StGB);
- die Verbreitung von Pornographie im Netz (§ 184 Ziffer 3 StGB);
- Abruf oder Besitz von Dokumenten mit kinderpornographischen Inhalten (§ 184 Ziffer 5 StGB);

- Ehrdelikte wie Beleidigung oder Verleumdung (§ 185 ff. StGB), Beschimpfungen von Bekenntnissen, Religionen oder Weltanschauungen (§ 166 StGB);
- Urheberrechtsverletzungen, z.B. durch die urheberrechtswidrige Vervielfältigung von Software oder die Erfassung geschützter Werke in einem IT-System (§§ 106 ff. UrhG), gleiches gilt auch für andere urheberrechtlich geschützte Werke (§ 2 UrhG).

3.2 Zulässige und unzulässige Nutzung

Ohne vorherige Zustimmung der MR-Systemtechnik dürfen keine Änderungen an der Konfiguration von IT-Systemen vorgenommen werden; im Übrigen gelten die Regelungen der Konzern-Betriebsvereinbarung zur Einführung und Verwendung von IT-Systemen. Sicherheitsvorschriften dürfen nicht umgangen werden, um Zugriff auf geschützte Daten bzw. geschützte Bereiche zu erlangen:

- Persönliche Benutzerkonten dürfen nicht gemeinsam mit anderen Benutzern verwendet werden. Jeder ist verantwortlich für den Schutz der auf seinem Benutzerkonto verwendeten bzw. gespeicherten Daten (z. B. benutzerspezifische Laufwerke, Outlook-Postfächer) und muss sich entsprechend mit den zulässigen Einsatzzwecken der IT-Systeme vertraut machen.
- Geräte mit Zugang zu unternehmenskritischen Informationen müssen bei Verlassen des Arbeitsplatzes durch geeignete Sperrmechanismen gesichert werden (z.B. passwortgeschützte Bildschirmschoner). Auf Dienstreisen müssen notwendige Vorkehrungen getroffen werden, um die Sicherheit der entsprechenden Gegenstände oder Unterlagen jederzeit gewährleisten zu können; die Ausrüstung muss als Handgepäck mitgeführt werden und darf nie unbeaufsichtigt bleiben. Mobile Geräte müssen, sofern diese nicht verwendet werden, an einem sicheren Ort aufbewahrt werden. Der Verlust bzw. Diebstahl von Geräten oder Daten ist unverzüglich beim zuständigen IT-Helpdesk anzuzeigen.

IT-Systeme des Reinhausen Konzern dürfen grundsätzlich nur im Rahmen der zugewiesenen Tätigkeit eingesetzt werden. Eine darüber hinaus gehende Nutzung ist im Rahmen der Konzern-Betriebsvereinbarung zur privaten Nutzung von Informations- und Kommunikationssystemen geregelt. Der Einsatz von IT-Systemen für Aktivitäten, die den Betrieb des Reinhausen Konzern beeinträchtigen oder stören, ist untersagt. IT-Systeme dürfen nicht für anstößiges oder unangebrachtes Material verwendet werden. Hierzu zählen insbesondere Hassbekundungen, sexuell ausgerichtetes, rassistisches oder diffamierendes Material.

4. Benutzerkonten

MR-Benutzerkonten müssen über eine Berechtigungsanforderung beantragt werden. Jedes Benutzerkonto ist durch ein sicheres Passwort bzw. durch weitergehende Authentifizierungsmaßnahmen geschützt. Sollten Administrationsrechte benötigt werden, wird ein zweites Benutzerkonto mit Sonderrechten erzeugt; normale Benutzerkonten dürfen nicht für Admin-Aufgaben genutzt werden. Jeder Mitarbeiter ist persönlich für den Schutz seiner Passwörter verantwortlich.

Konzernfremde können auch ohne Benutzerkonto per Gastzugriff (z.B. TEAMS, OneDrive, Sharepoint) der IT-Organisation beitreten; die eingeladenen Personen erhalten (automatisch) ein

befristetes Gastkonto im AZURE Active Directory. Benutzerkonten für Konzernfremde werden nur genehmigt, falls diese aus klar erkennbaren, geschäftlichen Gründen erforderlich sind und sich jeder Konzernfremde auf diese Konzernsicherheitsrichtlinie verpflichtet. Der Abschluss der Arbeiten ist vom Projektverantwortlichen dem IT-Helpdesk zu melden, damit das betreffende Benutzerkonto Betriebsfremder umgehend gelöscht werden kann.

Passwörter dürfen nicht an andere Personen weitergeben werden, auch nicht an den IT-Helpdesk. Ausnahmen bilden Gruppenkennungen, welche innerhalb einer Gruppe (z.B. Montage-Gruppen) bekannt sein müssen; diese Zugriffe sind auf das Minimum einzuschränken. Passwörter dürfen nicht in automatischen Anmeldeprozessen hinterlegt oder in einer Makro- oder Funktionstaste gespeichert werden. Passwörter müssen aus mindestens 8 Zeichen und aus mindestens drei der folgenden vier Zeichengruppen zusammengesetzt sein: Zahlen, Klein- und Großbuchstaben. Die IT-Systeme verifizieren die Korrektheit des eingegebenen Passwortes. Jedes Passwort muss spätestens nach 90 Tagen geändert werden. Bei wiederholt fehlerhafter Anmeldung wird das Benutzerkonto gesperrt; die Sperrung kann durch den Mitarbeiter mit Hilfe von MICROSOFT Authenticator selbständig behoben werden; dies gilt auch, wenn das Passwort vergessen wurde.

5. Softwarenutzung

Im Reinhausen Konzern dürfen nur legal lizenzierte Software-Programme eingesetzt werden, der Einsatz sogenannter „Raubkopien" ist streng verboten.

Ausschließlich die IT-Abteilung kann die Nutzung von Software genehmigen. Es ist untersagt, ohne Rücksprache mit der IT-Abteilung, Anwendungen zur Standardsoftware-Ausstattung hinzuzufügen (auch nicht aus Privateigentum) oder aus dieser zu entfernen. Das Herunterladen, Speichern oder Übertragen von Software aus dem Internet sowie der Einsatz von Share- oder Freeware-Programmen ist nur nach Freigabe durch den IT-Helpdesk erlaubt. Sollte verdächtige Software auf einem IT-System des Reinhausen Konzern entdeckt werden, muss dies unverzüglich dem IT-Helpdesk mitgeteilt werden. Daten und Informationen des Reinhausen Konzern dürfen nicht auf privaten Rechnern gespeichert oder verarbeitet werden; hiervon ausgenommen ist die Verwendung privater Endgeräte im Rahmen der „BYOD-Initiative" (Bring Your Own Device).

Es ist nicht gestattet, die IT-Systeme des Reinhausen Konzern zum Herunterladen, Speichern, Vertreiben oder Erstellen von Kopien illegaler, urheberrechtlich geschützter oder nicht lizenzierter Software, Daten, Musik oder anderer Multimediadaten zu nutzen (siehe hierzu auch Ziffer **Fehler! Verweisquelle konnte nicht gefunden werden.**). Es ist nicht gestattet, Anwendungen, die dem Aufspüren von Sicherheitsschwachstellen oder dem Ausspähen von Daten (z.B. Hacking-Tools) dienen, einzusetzen.

6. Schadsoftware

Computerviren, Trojaner und andere bösartige Programme stellen eines der größten Risiken für die Informationssicherheit dar. Bei der Bekämpfung solcher Programme verfolgt der Reinhausen Konzern eine restriktive und vorausschauende Strategie.

Auf jedem IT-System des Reinhausen Konzern wird eine Antivirensoftware ausgeführt; Updates für den Virenscanner werden in regelmäßigen Intervallen über das Netzwerk bereit gestellt. Es ist untersagt, die Aktualisierung und Ausführung der Antivirensoftware zu deaktivieren oder deren ordnungsgemäße Funktion zu behindern. Der IT-Helpdesk ist zu benachrichtigen, sofern die Software nicht ausgeführt wird oder nicht mehr aktuell ist (z.B. durch eine Warnmeldung des Antiviren-Programms). Auf den E-Mail-Servern ist ein Antivirenprogramm für die Überprüfung aller eingehenden und ausgehenden E-Mail-Nachrichten implementiert – trotzdem dürfen Anhänge in E-Mail-Nachrichten von unbekannten Absendern nicht ohne Rückfrage beim IT-Helpdesk geöffnet werden. Der IT-Helpdesk ist unverzüglich zu benachrichtigen, sobald auch nur vermutet wird, dass ein IT-System des Reinhausen Konzern von einem Virus oder einem bösartigen Programm infiziert wurde.

7. E-Mail-Nutzung

7.1 Zulässige und unzulässige Nutzung

Der Reinhausen Konzern ist bestrebt, für alle Mitarbeiter und Kommunikationspartner ein benutzerfreundliches, rechtskonformes und sicheres E-Mail-System bereitzustellen. Um dessen hohe Verfügbarkeit und Zuverlässigkeit sicherzustellen, ist die Einhaltung bestimmter Regeln im Zusammenhang mit E-Mails erforderlich. Die Nutzung des vom Reinhausen Konzern zur Verfügung gestellten E-Mail-Kontos ist grundsätzlich nur für dienstliche Zwecke erlaubt. Jeder Mitarbeiter ist dafür verantwortlich, dass seine Benutzerkonto-Informationen, insbesondere das gewählte Passwort, geheim bleiben. Benutzer tragen die Verantwortung für sämtliche Aktivitäten, die über deren E-Mail-Konto abgewickelt werden.

E-Mails für externe Empfänger sind mit einer Signatur zu versehen; eine Vorlage findet sich im GroupNet. Die jeweilige Führungskraft ist über jeden Verdacht der unbefugten Nutzung eines Benutzerkontos oder Passwortes zu informieren. Sämtliche E-Mail-Nachrichten, welche unternehmenskritische Informationen enthalten, müssen entweder über sichere Verbindungen übertragen (MR-LAN, VPN oder angeschlossene Tochtergesellschaften) oder vor dem Senden mit WinZip verschlüsselt werden (eine Beschreibung findet sich im GroupNet).

Eine WLAN-Verbindung via VMware stellt eine sichere Verbindung dar. Dennoch müssen bei der Verwendung von E-Mails Risiken aus Viren oder gefährlichen Codes beachtet und entsprechende Sicherheitsvorkehrungen ergriffen werden:

- Eingehende und ausgehende E-Mails werden auf unerlaubte Anhänge geprüft und gegebenenfalls nicht zugestellt. Eine Liste, der aktuell nicht zulässigen Dateitypen kann im GroupNet eingesehen werden.
- E-Mail-Anhänge und Hyperlinks, die vermeintlich oder gar nachweislich Viren bzw. andere potenziell schädliche Inhalte aufweisen, dürfen nicht geöffnet werden. Benutzer müssen sich zum weiteren Vorgehen mit den Mitarbeitern des IT-Helpdesks in Verbindung setzen. Auch Viruswarnungen dürfen nur an den IT-Helpdesk weitergeleitet werden.
- Benutzer dürfen nicht leichtfertig auf Nachrichten unbekannter Absender antworten (Ausnahme: Abwesenheitsassistent) – oftmals versuchen Dritte hierdurch an authentische Benutzersignaturen zu kommen.

- Postfächer (Posteingang inkl. Spam-Ordner) sollten mindestens einmal pro Arbeitstag überprüft werden. Sollte dies nicht möglich sein (Abwesenheit, Urlaub etc.), so ist in jedem Fall eine automatische E-Mail-Antwort (Abwesenheitsassistent) zu aktivieren und gegebenenfalls eine Stellvertreterregelung im E-Mail-System einzurichten. Die Abwesenheitsnotiz muss den Zeitraum der Abwesenheit sowie den Stellvertreter benennen und einen Vermerk enthalten, falls die E-Mail nicht weitergeleitet wird; Vorlagen finden sich im GroupNet.
- Bei längerer Abwesenheit des Benutzers (z.B. Krankenhausaufenthalt nach einem Unfall) erhält dessen Führungskraft nach Einbindung des Betriebsrats per schriftlicher Anforderung an den zuständigen IT-Helpdesk und Genehmigung durch den zuständigen Bereichsleiter (z.B. Berechtigungsanforderung) Leseberechtigung zum Postfach; dieser Zugang wird für den Benutzer protokolliert.

E-Mail-Systeme des Reinhausen Konzern dürfen nicht für die Übermittlung von nicht angemessenem, anstößigem, bedrohendem, illegalem oder belästigendem Material zu nutzen. Es darf kein illegales, diskriminierendes oder urheberrechtlich geschütztes Material gespeichert oder versandt werden. E-Mail-Konten dürfen nicht zum Senden inoffizieller, unerwünschter Nachrichten (Spam) an eine große Gruppe von Personen verwendet werden. Es ist untersagt, E-Mail-Konten für geschäftliche Aktivitäten von nicht mit MR verbundenen Unternehmen oder Personen zu nutzen. Im Übrigen wird auf Ziffer 3 verwiesen.

7.2 Gruppenpostfächer

Benutzer dürfen das persönlich zugewiesene E-Mail-Konto nicht mit einem anderen Benutzer gemeinsam betreiben. Bei Vertretungs- oder Assistenzregelungen muss der Zugriff über Stellvertreter-Funktion des E-Mail-Programms erfolgen und nicht durch Weitergabe des persönlichen Passworts.

Gruppenpostfächer sind explizit zur gemeinsamen Nutzung durch mehrere Mitarbeiter freigegeben. Der Versand von E-Mails ist nur an Empfänger innerhalb des Reinhausen Konzern möglich.

8. Internet-Nutzung

8.1 Zulässige Nutzung

Die Nutzung des Internets beinhaltet Gefahren (z.B. Ausspähen lokaler Daten, Virenbefall), der durch geeignetes Nutzerverhalten zu begegnen ist. Das Internet darf grundsätzlich nur zu geschäftlichen Zwecken genutzt werden.

8.2 Unzulässige Nutzung

Benutzer müssen sich mit den Risiken der Internet-Nutzung vertraut machen. Zum Schutz der Interessen des Reinhausen Konzern sind folgende Nutzungen untersagt:

- das Herunterladen bzw. Installieren von nicht von der IT freigegebener Software aus dem Internet;
- das Veröffentlichen vertraulicher Informationen bzw. unternehmenskritischer Daten über den Reinhausen Konzern, deren Kunden und Lieferanten;

- der Zugriff auf illegales/anstößiges Material (Anzeigen, Herunterladen, Vertreiben – Kapitel 3);

Ausnahmen hiervon, die zur Erfüllung des Arbeitsauftrages nötig sind, werden von der Führungskraft in Rücksprache mit dem Konzernsicherheitsbeauftragten oder – soweit es das Herunterladen bzw. Installieren von Software aus dem Internet betrifft – in Rücksprache mit der IT genehmigt.

9. Telekommunikation

Das Telefonsystem sowie die zur Verfügung gestellten Mobiltelefone sind für dienstliche Zwecke zu nutzen. Zulässigkeit und Umfang einer privaten Nutzung von IT-Systemen werden per Betriebsvereinbarung geregelt. Nachrichten, die unternehmenskritische Informationen enthalten, dürfen nicht auf Anrufbeantwortern oder Voicemail-Systemen hinterlassen werden. Gespräche mit unternehmenskritischen Informationen dürfen nicht aufgezeichnet werden.

Benutzer sind aufgefordert, stets die Identität eines Anrufers oder einer Person zu überprüfen, die Informationen anfordert, um sicherzustellen, dass Unbefugte nicht in den Besitz kritischer Informationen gelangen können. Darüber hinaus dürfen Dritte nur mit Zustimmung des Benutzers dem Gespräch folgen (Lautsprecher, Freisprecheinrichtungen etc.). Alle vermuteten oder erkannten Ausspähversuche sind umgehend an den IT-Helpdesk zu melden.

10. Sicherer Umgang mit Daten und Datenträgern

Die Verwendung externer Datenträger (USB-Stick, CD usw.) birgt Gefahren. Durch Datenträger können Schadsoftware von Dritt-Systemen auf die IT-Systeme des Reinhausen Konzern übertragen werden oder unerkannt Informationen von diesen abgezogen werden. Daher dürfen nur Datenträger (Produkte) verwendet werden, die von dem Reinhausen Konzern bereitgestellt bzw. beschafft wurden.

Geschäftsrelevante Daten müssen zur Ermöglichung einer automatischen Datensicherung auf zentralen IT-Systemen gespeichert werden. Lokal abgelegte Daten (z.B. auf Laptops) werden nicht automatisch gesichert – hierfür muss der Benutzer durch Nutzung externer Datenträger selbst Sorge tragen (z.B. auf Dienstreisen ohne Netzwerk-Zugang).

11. Externer Zugriff auf IT-Systeme des Reinhausen Konzern

Der Zugriff von einem Arbeitsplatz außerhalb des Reinhausen Konzern auf das interne IT-System (Remote-Zugang) stellt einen der kritischsten Angriffspunkte für Unbefugte dar. Für diesen Fall wurden besondere Schutzvorkehrungen getroffen (VPN-Access und Outlook Web Access):

- die Autorisierung eines Remote-Zugangs kann bei berechtigtem Interesse mit Einverständnis der Führungskraft bei der IT-Abteilung per Berechtigungsanforderung beantragt und von dieser ein Authentifizierungs-Tools bereitgestellt werden;
- es ist nicht gestattet, Benutzerkonten, Passwörter bzw. PINs für den Remote-Zugang mit anderen Personen gemeinsam zu nutzen, auch darf keine zusätzliche Hardware installiert werden, um den

genehmigten Zugangspunkt zu umgehen, ebenso dürfen keine Remote-Tools für den Remote-Zugang von anderen Netzwerken aus installiert werden;
- bei Nutzung eines VMware-Zugangs dürfen keine Dateien des lokalen Systems (Festplatte, Laufwerk C:) in das Netzwerk des Reinhausen Konzern hochgeladen werden.

12. Datenschutz

Betrieb und Sicherheit von IT-Systemen berühren häufig auch den Schutz personenbezogener Daten (Datenschutz). Die Datenschutzbeauftragten prüfen die Einhaltung datenschutzrechtlicher Vorschriften und bezüglich dieser Konzernsicherheitsrichtlinie Teil des Sicherheitsmanagements (Kapitel 2). Durch die Nutzung von IT-Systemen des Reinhausen Konzern erklären sich die Benutzer mit der Überwachung und Protokollierung der Nutzung einverstanden.

Die Systemadministratoren können mit Hilfe automatisierter Überwachungsverfahren eine unsachgemäße Nutzung der IT-Systeme feststellen. Soweit dabei personenbezogene Daten aufgezeichnet werden, dienen diese ausschließlich zur Gewährleistung der Systemsicherheit, zur Optimierung und Steuerung der IT-Systeme, zur Fehleranalyse und -korrektur sowie zur kostenstellenbezogenen Abrechnung (analog Art. 5 DSGVO). Zugriffe bleiben auf die Systemadministratoren begrenzt, welche wiederum auf die Einhaltung des Datenschutzes verpflichtet sind (analog Art. 24, 29, 32 DSGVO).

Der Reinhausen Konzern setzt Kameras und andere elektronische Geräte für die Überwachung von Aktivitäten in sicherheitskritischen Bereichen ein. Der Reinhausen Konzern beachtet die Privatsphäre von Mitarbeitern und wird keine Videoüberwachungen in besonders schützenswerten Bereichen, insb. Sanitärbereiche und Umkleideräume vornehmen. Weiterhin werden Systeme eingesetzt, die den Zutritt zu bestimmten Bereichen auf hierzu autorisierte Personen beschränken; der erfolgreiche Zutritt zu diesen Bereichen sowie erfolglose Versuche, sich Zutritt zu diesen Bereichen zu verschaffen, werden protokolliert.

Unternehmenskritische Daten (z.B. Produkt-, Finanz-, Kunden-, Prozessdaten sowie Technologie- und Strategieunterlagen) sind besonders schützenswert; die Offenlegung dieser Informationen an Unbefugte (z.B. Wettbewerber) kann großen Schaden zufügen. Derartige vertrauliche Informationen – aber auch Kundendaten und Informationen zu Personen – dürfen daher, wenn überhaupt, nur mit dienstlicher Veranlassung, der Zustimmung des für diese Informationen Verantwortlichen und erforderlichenfalls des Datenschutzbeauftragten an hierzu Berechtigte weitergeben werden.

13. Physische Sicherheit

13.1 Zutritt zu Gelände und Gebäuden

Insbesondere der physische Schutz (z.B. Gebäude, IT-Systeme) trägt zur Steigerung der Sicherheit von Beschäftigten und Unternehmens bei. Zutritt zu Betriebsgelände und -gebäuden erhalten Belegschaftsangehörige ausschließlich über den dafür vorgesehenen Personalzugang und den codierten Firmenausweis. Verlust/Diebstahl von Ausweisen/Schlüsseln, welche den Zutritt zu Gebäuden ermöglichen, sind unverzüglich dem jeweiligen Empfang bzw. der Standortleitung zu melden.

Auf dem Firmengelände und in Gebäuden des Reinhausen Konzern sind Firmenausweise gut sichtbar zu tragen, soweit dies nicht der Arbeitssicherheit widerspricht (z.B. in der Produktion). Beim Verlassen des Firmengeländes ist der Ausweis abzunehmen und sicher vor Einsichtnahme Dritter, Beschädigung, Verlust oder Diebstahl zu verwahren. Schlüssel und Ausweise dürfen nur vom Empfang gegen Empfangsprotokoll an auf dem Betriebsgelände tätige Dritte ausgeben werden.

13.2 Arbeitsplatz und Besprechungsräume

Die Fenster sämtlicher Räumlichkeiten müssen bei Arbeitsende geschlossen werden; dies gilt insbesondere auch für Besprechungsräume. Portable Geräte (z.B. Laptop, Smartphone) sind auch auf dem Firmengelände – insbesondere während Arbeitspausen – für Unbefugte zu sperren sowie gegen Diebstahl zu schützen; der Verlust oder Diebstahl von Endgeräten ist unverzüglich beim IT-Helpdesk anzuzeigen. Insbesondere sind die notwendigen Vorkehrungen zu treffen, um die Möglichkeit des Ausspähens sicherheitsrelevanter Daten (z.B. Passwörter) zu verhindern. Bei Arbeitsende ist der PC herunterzufahren, Peripheriegeräte sind auszuschalten.

Vor jeder Besprechung müssen Vorkehrungen getroffen werden, um zu vermeiden, dass Unbefugte durch geöffnete Fenster oder Türen Kenntnis von unternehmenskritischen Informationen erhalten; dies gilt insbesondere auch für virtuelle Besprechungen. Vertrauliche Sachverhalte dürfen nur an Orten erörtert werden, welche einen entsprechenden Schutz vor unbefugten Zuhörern bieten. Zudem ist sicherzustellen, dass keine unternehmenskritischen Informationen im Besprechungsraum zurückgelassen werden (z.B. auf Whiteboards, Flipcharts, in Form liegengelassener Unterlagen).

13.3 Sicherheits-, Überwachungs-, und Schutzsysteme

Um Bereiche und Räume mit sensiblen Systemen, Anlagen und Informationen vor Einbruch/Sabotage zu schützen, sind an verschiedenen Stellen auf dem Betriebsgelände Überwachungseinrichtungen installiert. In besonderen Fällen erfolgt zudem ein Schutz vor Brandschäden durch Feuerlöschsysteme. Ein Alarm der Überwachungs- und Brandmeldeanlagen wird automatisch am Empfang (oder einer anderen Stelle) gemeldet; sollte ein derartiges Schutzsystem erkennbar nicht funktionieren, ist unverzüglich der Empfang bzw. die Standortleitung zu informieren.

13.4 Fotografier- und Aufzeichnungsverbot

Auf dem Firmengelände und in den Gebäuden des Reinhausen Konzern herrscht für Mitarbeiter sowie insbesondere für Betriebsfremde ein generelles Fotografier- und Aufzeichnungsverbot betreffend Bild und Ton. Ausnahmen bedürfen der Genehmigung des Standortleiters, ersatzweise des Konzernsicherheitsbeauftragten. Genehmigungsfrei bleiben Aufnahmen zur Digitalisierung von Aufzeichnungen wie Flipcharts / Whiteboards für die rein dienstliche Verwendung.

14. Besucherregelungen

Durch die folgenden Besucherregelungen wird sichergestellt, dass die Einrichtungen des Unternehmens nicht ohne explizite Berechtigung betreten werden können.

- Nur hierzu explizit autorisierte Personen dürfen das Betriebsgelände des Reinhausen Konzern betreten. Alle anderen Personen müssen sich am Empfang mit folgenden Daten in der Besucherverwaltung registrieren lassen: Name und Firma des Besuchers, Kontaktperson in dem Reinhausen Konzern, Datum und Uhrzeit des Besuchs. Besucher sind geeignet auf erwünschtes Verhalten, insbesondere auf das generelle Fotografier- und Aufzeichnungsverbot hinzuweisen.
- Besucher erhalten einen Besucherausweis, welcher während des Aufenthalts auf dem Betriebsgelände gut sichtbar an der Kleidung getragen und beim Verlassen des Betriebsgeländes wieder zurückzugeben ist.
- Eine Ausnahme besteht bei geführten Gruppen (z.B. Schulklassen, Studentengruppen). Diese können sich ohne Ausgabe von Besucherausweisen auf dem Betriebsgelände bewegen, sofern die Gruppe sich in ständiger Begleitung eines Mitarbeiters des Reinhausen Konzern befindet.
- Dienstleister, welche auf dem Betriebsgeländer Arbeiten verrichten, erhalten von der auftraggebenden Kontaktperson eine Autorisierung, sich erforderlichenfalls unbegleitet auf dem Betriebsgelände zu bewegen – hierfür wird ein besonders gekennzeichneter Besucherausweis ausgestellt; für Dienstleister mit regelmäßigem Einsatz auf dem Betriebsgelände besteht die Möglichkeit zur Erteilung einer Jahresfreigabe.
- Werden Besucher oder unbekannte Personen unbegleitet und/oder ohne gültigen Besucherausweis angetroffen, so sind diese anzusprechen und zum Empfang zu geleiten; bei Widerstand seitens der Besucher ist umgehend der Empfang bzw. die Standortleitung zu informieren.

In Notfällen ist dem Fachpersonal Zugang zum Betriebsgelände zu gewähren. Sanitäter, Feuerwehr und/oder Polizei sind auf dem Werksgelände zu begleiten; der Empfang ist zu informieren.

15. Sicherheitstraining und Ansprechpartner

Die Umsetzung dieser Konzernsicherheitsrichtlinie wird durch ergänzende Informationen, Kampagnen und (Schulungs-) Veranstaltungen (u.a. im GroupNet) unterstützt. Ansprechpartner für Notfall-Situationen finden sich im GroupNet. Fragen zur Sicherheit, zum Datenschutz und/oder zu dieser Konzernsicherheitsrichtlinie können jederzeit an sicherheit@reinhausen.com (bzw. security@reinhausen.com) gerichtet werden, auf welche die Mitglieder des Konzernsicherheitsteams gleichberechtigten Zugriff haben.

16. Anlagen

Die nachfolgenden Dokumente sind Bestandteil dieser Konzernsicherheitsrichtlinie und sind im GroupNet abgelegt:

Anlage 1: Konzernrichtlinie zur Klassifizierung und Handhabung von Informationen
Anlage 2: Compliance Response Plan
Anlage 3: Handlungsleitfaden zum Verhalten bei Durchsuchungen

Regensburg, den 14.07.2023

Geschäftsführung Konzernsicherheitsbeauftragter
Maschinenfabrik Reinhausen GmbH

Glossar

Angriff	Versuch, die Verwundbarkeit eines System auszunutzen oder zu suchen
Authentifizierung	Überprüfen einer Identität.
Authentizität	Überprüfte und bestätigte zweifelsfreie Herkunft bzw. Identität.
Autorisierung	Erteilte Berechtigung.
BDSG-neu	Bundesdatenschutzgesetz
Bedrohung	Umstand, der direkt oder indirekt zu einem Schaden/Sicherheitsverlust führen kann.
Benutzerkonto	Ein Benutzerkonto (user account) ist eine Zugangsberechtigung zu einem zugangsbeschränkten IT-System. Üblicherweise muss ein Anwender sich beim Login mit Benutzername und Passwort (Kennwort) authentisieren. Einem Benutzerkonto können verschiedene Privilegien zugeordnet werden, zum Beispiel Zugriffsrechte.
Benutzungsberechtigung	Berechtigung zur Nutzung von Computerdiensten (Mail, Internet etc.).
Daten	Gebilde aus Zeichen zur Abbildung von Informationen und Medien (Sprache, Bilder), die gespeichert oder verarbeitet werden.
DoS-Attacke	Angriff auf die IT-Sicherheit mit dem Ziel, bestimmte Dienste oder auch nur einen Rechner vollständig zu blockieren (Denial of Service).
DNS	Das Domain Name System dient der Beantwortung von Anfragen zur Namensauflösung in IP-basierten Netzwerken.
Download	Herunterladen einer Datei von an anderen Orten betriebenen Rechnern mit Hilfe eines Übertragungsprotokolls; der umgekehrte Vorgang heißt Upload.
DSGVO	Datenschutzgrundverordnung
Firewall	Zugangsschutzsystem zur organisatorisch-technischen Trennung von Netzbereichen in einem Rechner-Netzwerk. Firewalls sitzen an den Schnittstellen zwischen einzelnen Teilnetzen und kontrollieren den Netzwerkverkehr, um unerwünschte Vorgänge verhindern und nur den erwünschten Datenverkehr zu ermöglichen,
Hacker	Personen, die in fremde Rechner eindringen (wollen), um Daten auszuspähen. Hacking/Cracking wird auch als Einbrechen bezeichnet.
Hyperlink	Elektronischer Querverweis in einem Text, der funktional u.a. einen Sprung zu einem anderen elektronischen Dokument im eigenen Netzwerk oder auch im World Wide Web bewirkt.
Informationen	Im Rahmen von Geschäftsabläufen entscheidungsrelevante Daten.

Informationstechnik- bzw. Informations- und Kommunikationstechnik-Systeme (IT- bzw. IuK-Systeme)	Informational Technology (IT): Umfasst E-Mail-Systeme, Internet (http/https, ftp), Rechner-Netzwerke, Telefonie (Funk, Mobiltelefone, Smartphones etc.), Server, Arbeitsplatzcomputer (PC, Laptops, Tablets, Handhelds), Speichermedien (USB-Sticks, SD-Karten, externe Festplatten, CD-RW, Disketten etc.), Scanner, Digitalkameras, Tonaufzeichnungsgeräte (mp3-Player, Minidisc-Player, Kassettenrecorder, Radio), sonstige Hardware zur Datenübertragung (Modem, Kabel, Switch, Hub).
Integrität	Eigenschaft, dass IT-Systeme und Daten, die gespeichert, verarbeitet oder übertragen werden, ausschließlich zulässigen Veränderungen unterlagen.
IP	Internet Protocol: Auf dieser Basis ist es möglich, Computer in größeren Netzwerken zu adressieren (IP-Adresse) und an diese sog. IP-Pakete zu senden. Die logische Adressierbarkeit von Teilnehmern ist die Grundlage für das sog. Routing (Wegewahl und Weiterleitung von Netzwerk-Paketen).
IT-Sicherheit bzw. -Sicherheitsmanagement	Fachgebiet, welches sich mit der Sicherheit von IT-Prozessen sowie der Erfassung und Minimierung von Risiken befasst. IT-Sicherheit entsteht aus einem sinnvollen Zusammenspiel von technischen und organisatorischen Maßnahmen.
Kettenbrief	Dabei handelt es sich meist um Mails mit der Aufforderung, Bekannte anzuschreiben und diesen den Inhalt der Mail bekannt zu geben. Meist wird vor Viren gewarnt, welche dann gar keine sind (Hoaxe), es wird um Unterschriften zu einem Ereignis gebeten, es wird der Anschein von Gewinnen erzeugt usw. – es handelt sich also um Mails ohne ernsthaften Hintergrund.
Mail Bomb	Hierunter versteht man das automatisierte Bombardieren eines Mail-Servers mit E-Mails, um über das Ausschöpfen der Kapazitäten des Rechners den Totalausfall des Systems zu provozieren.
Mail Header	Vorangestellter Teil einer Mail, welcher administrative Informationen enthält (Adresse des Absenders, Versanddatum der Nachricht etc.).
MP3	Teil des MPEG-Standards (Moving Picture Experts Group) zur digitalen Kompression von Audio- und Videosignalen, wie diese heute im digitalen Rundfunk und im Internet eingesetzt werden. MP3 erlaubt die Kompression von Musiksignalen auf ca. 8 % der sonst notwendigen Bitrate und dies nahezu ohne hörbare Unterschiede zum Originalsignal.
Nachweisbarkeit	Verbindlicher Nachweis, so dass die an Veränderungen Beteiligten über keinerlei Mittel verfügen, ihre Beteiligung zu bestreiten.

Netiquette	Ungeschriebene Gesetze über das Verhalten im Internet (z.B. in Chatrooms). Diese sollen den freizügigen Datenverkehr wahren und zu einem verantwortungsbewussten Agieren im Netz beitragen (z.B. keine radikale/obszöne Inhalte öffentlich verbreiten, Urheberrecht beachten).
OT-Systeme	Operational Technology (OT): Umfasst alle Einrichtungen (Hardware und Software) zur Überwachung und Steuerung industrieller Prozesse.
Passwort	Zeichenkette, die als Authentifizierungsinformation dient.
Portscan	Das Abfragen (scannen) von Ports (Schnittstellen zu Internetzugängen von Firmennetzen oder einzelnen Computern) mit dem Ziel, den Zugangscode zu ermitteln, um sich unberechtigten Zugang in fremde Netze/Computer zu verschaffen.
Restrisiko	Potentielle IT-Schäden, die aus technischen, organisatorischen oder finanziellen Gründen nicht oder nur mit unverhältnismäßigem Aufwand vermieden und insofern bewusst in Kauf genommen werden.
Sniffer Tools	Beim Hochfahren eines Arbeitsplatzrechners gibt eine Client-Software die aktuell erkannte Hard- und Software-Konfiguration an eine Server-Software weiter, welche diese in einer Datenbank speichert (z.B. MICROSOFT SMS).
Spam	Abgeleitet von "Spiced Pork And haM" ("Frühstücksfleisch" aus einem Monty Python-Sketch): Der Netiquette widersprechende Nutzung von E-Mail für Rundsendungen (z.B. Wurfsendungen in elektronischer Form, die durch sog. "make money fast"-Anbieter an viele, nicht daran interessierte Empfänger gesendet werden).
Spoofing	Das Einfügen einer falschen IP-Absenderadresse in eine Internet-Übertragung. Das Ziel dieser Aktion ist der unberechtigte Zugriff auf ein Computersystem. Vortäuschen eines falschen Absenders von IP-Paketen (IP-Spoofing), eines anderen Domain-Namens (DNS-Spoofing) oder des gesamten World Wide Web durch Umleitung von Anfragen über einen Zwischenrechner (Web-Spoofing)
Trojaner	Sabotage-Programme, die sich wie normale Software verhalten (dem Benutzer werden normale Programmaktionen vorgetäuscht), aber Anweisungen enthalten, die Schaden anrichten können (und für den Benutzer verborgen im Hintergrund ablaufen).
Verfügbarkeit	Gewährleistung der Durchführung genehmigter Zugriffe und Veränderungen auf Daten und Systeme innerhalb einer definierten Zeit.
Vertraulichkeit	Gewährleistung, dass nur berechtigten Nutzern der Zugang zu einem definierten Zweck ermöglicht wird.

VPN	Virtual Private Network (virtuelles privates Netz): Dient der sicheren Einbindung von Geräten eines benachbarten Netzes an das eigene Netz, ohne dass die Netzwerke zueinander kompatibel sein müssen.
Worms	Sabotage-Programme, die im Gegensatz zu Viren unabhängig von anderen Programmen laufen (Worms benötigen keine Wirtsprogramme) und sich selbstständig in einem Netzwerk ausbreiten können.
Zugangsberechtigung	Umfasst alle Maßnahmen zur Regelung des Netzwerkzugangs. Einfachste Form der Reglementierung ist die Vergabe von Passwörtern und Benutzernamen. Darüber hinaus können Zeit- oder Anwendungsbeschränkungen vergeben werden.