AlbatrossProjects

Informationssicherheitsleitlinie

Firma
Albatross Projects GmbH
Daimlerstrasse 17
89564 Nattheim

INFORMATIONSSICHERHEITSLEITLINIE

Ordnungsschlüssel:	VA-GU-00001
Ablageort:	IMS
Version:	1.0
Referenzdokumente:	3.0 - 41 Informationssicherheitsleitlinie
Datum der Version:	08.05.2023
Revision Intervall:	12 Monate
Erstellt durch:	M. Schuster
Geprüft durch:	B. Kienle
Genehmigt durch:	Geschäftsleitung
Genehmigt am:	01.06.2023
Vertraulichkeitsstufe:	1

ÄNDERUNGS-HISTORIE

Datum	Version	Erstellt durch	Beschreibung der Änderung
21.04.2023	1.0	MSR	Erster Entwurf des Dokuments
08.05.2023	1.0	BK	Anpassung Dokument

Inhalt

1. ZWECK UND ANWENDUNGSBEREICH

Unsere betrieblichen Prozesse werden immer mehr durch die Informationstechnologie unterstützt, was jedoch auch bedeutet, dass wir zunehmend von dieser abhängig sind. Um unsere Prozesse und Datenverarbeitungssysteme sowie die IT-Infrastruktur und Datenbestände vor Gefahren wie Missbrauch, Schadsoftware, Spionage und Fehlbedienungen zu schützen, haben wir eine Richtlinie mit entsprechenden Maßnahmen entwickelt. Diese Maßnahmen sollen sicherstellen, dass die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität eingehalten werden. Weitere Informationen und Details zu unseren Zielen sind in unserem "IT-Security Konzept" zu finden.

2. GELTUNGSBEREICH UND ZIELE

Die vorliegende Richtlinie gilt uneingeschränkt für alle Beschäftigten der Albatross Projects GmbH, einschließlich derjenigen, die im Rahmen von Montagearbeiten tätig sind, sowie für diejenigen, die von zu Hause ausarbeiten. Darüber hinaus gilt sie auch für externe Mitarbeiter, die möglicherweise in Projektgeschäft tätig sind. Für externe Mitarbeiter muss gegebenenfalls sichergestellt werden, dass sie die Bestimmungen dieser Richtlinie einhalten, entweder durch entsprechende Verpflichtungserklärungen oder vertragliche Regelungen. Die Richtlinie gilt für alle Arten von Hard- und Software sowie für sämtliche im Unternehmen eingesetzten Datenverarbeitungsverfahren und mobilen Datenträger, einschließlich derjenigen, die von externen Stellen verwaltet werden. Dies schließt beispielsweise Laptops, Tablets, Smartphones und USB-Sticks ein. Sollten in Ausnahmefällen abweichende Verfahrensweisen erforderlich sein, so dürfen diese nur nach vorheriger Genehmigung durch die Geschäftsleitung umgesetzt werden. Es ist von entscheidender Bedeutung, dass alle Beschäftigten, einschließlich externer Mitarbeiter, diese Richtlinie vollständig verstehen und einhalten, um die Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit der Daten des Unternehmens zu gewährleisten. Durch die Einhaltung dieser Richtlinie können potenzielle Sicherheitsrisiken minimiert und ein sicherer Umgang mit den Daten des Unternehmens gewährleistet werden.

3. ORGANISATION

Zum Erreichen der Informationssicherheit -und Datenschutzzeile wird eine Sicherheitsorganisation eingerichtet. Dafür wurde ein externer Berater beauftragt. Dieser unterstützt die Verantwortlichen und ist die Ansprechstelle für alle Beschäftigten des Unternehmens in Fragen der Informationssicherheit und des Datenschutzes.

Die Kontaktdaten sind im Unternehmen veröffentlicht.

4. ALLGEMEINE REGELUNGEN

4.1 Zweckbindung der Systeme und Arbeitsmittel

Albatross Projects GmbH stellt sämtliche IT-Einrichtungen wie PCs, Notebooks, USB-Sticks, Speicherkarten und mobile Laufwerke sowie andere mobile Geräte wie PDAs, Tablets usw. für geschäftliche Zwecke zur Verfügung und diese unterliegen den Bestimmungen dieser Richtlinie. Die Beschaffung von IT-Ausrüstung für den Einsatz im Unternehmen ist nur nach Prüfung und Genehmigung durch die IT-Abteilung und gemäß den festgelegten Spezifikationen zulässig. Die Verwendung von Hard- und/oder Software, die nicht gemäß den festgelegten Spezifikationen beschafft und eingerichtet wurde, ist unzulässig. Ausnahmen können nur nach Absprache mit den zuständigen Stellen und schriftlicher Dokumentation gemacht werden. Bevor jegliche Art von Hard- und Software in Betrieb genommen wird, muss sie von der zuständigen Abteilung technisch und gegebenenfalls von den zuständigen Stellen fachlich genehmigt werden. Die Genehmigungen müssen dokumentiert werden. Die Nutzung von nicht genehmigter Software, insbesondere organisationsfremder IT-Dienste, ist unzulässig. Veränderungen sind nur auf Anforderung der zuständigen Stelle zulässig und müssen dokumentiert werden.

4.2 Mobiles Arbeiten

Um die Sicherheit vom mobilen Arbeiten zu gewährleisten, insbesondere im Hinblick auf den Schutz vertraulicher Daten und Informationen stellen wir sicher, dass alle Mitarbeiter sich an festgelegte Bestimmungen in Form von Richtlinien halten.

4.2.1 Mobile Kommunikationsgeräte

Um Verluste von Firmendaten zu vermeiden, ist es notwendig, dass auf Notebooks und mobilen Kommunikationsgeräten wie Mobiltelefonen und PDAs lediglich Kopien der Daten gespeichert werden. Sollten dabei personenbezogene oder andere vertrauliche Daten gemäß den Vorschriften der Vertraulichkeitsrichtlinie gespeichert werden, müssen diese verschlüsselt werden.

Folgende Vorsichtsmaßnahmen sind zu beachten:

- Die Festplatten von portablen Geräten wie Notebooks müssen mit Bitlocker verschlüsselt werden.
- Jedes mobile Gerät muss durch ein sicheres Passwort gemäß dieser Richtlinie oder durch ein anderes sicheres und zugelassenes Verfahren geschützt werden.
- Es muss sichergestellt werden, dass unbefugte Personen keinen Zugang zu privaten Räumen haben.
- Es ist nicht erlaubt, Notebooks an unbefugte Personen weiterzugeben oder sie von Familienmitgliedern nutzen zu lassen.

- Wenn Notebooks von verschiedenen Benutzern oder in unsicheren oder unbekannten Umgebungen eingesetzt werden, müssen sie regelmäßig auf Sicherheitsrisiken überprüft werden.
- In öffentlichen Räumen, wie Verkehrsmitteln müssen Blickschutzfilter verwendet werden, um eine unberechtigte Verarbeitung von personenbezogenen oder anderen sensiblen Daten zu verhindern.
- Mobile Geräte dürfen nicht unbeaufsichtigt gelassen und müssen sicher aufbewahrt werden.
- Es ist nur erlaubt, mobile Geräte ohne personenbezogene oder vertrauliche Daten an fremde Rechner anzuschließen.
- Nach dem Anschluss an fremde Rechner müssen die mobilen Geräte auf Viren und andere Schadsoftware geprüft werden.

4.2.2 Verhalten und Arbeiten in fremden Umgebungen

Um sicherzustellen, dass keine Datenverluste auftreten, sollte darauf geachtet werden, dass auf Notebooks und mobilen Kommunikationsgeräten wie Mobiltelefonen oder PDAs nur Kopien von Firmendaten gespeichert werden. Falls personenbezogene Daten oder andere vertrauliche oder streng vertrauliche Daten gemäß der Dokumentenlenkung gespeichert werden müssen, sollten diese Daten verschlüsselt werden, um ihre Sicherheit zu gewährleisten.

Wenn man auf Reisen ist, sollten Notebooks und andere mobile Datenträger niemals unbeaufsichtigt gelassen werden, auch nicht in Zügen oder bei Sicherheitskontrollen an Flughäfen oder anderen öffentlichen Orten. Es wird vermieden, Notebooks als aufgegebenes Gepäck auf Flügen mitzunehmen oder sie sichtbar im Auto liegen zu lassen. Wenn ein Taxi oder ein Mietwagen genutzt wird, sollten Datenträger nicht im Fahrzeug zurückgelassen werden. Bei Mitnahme eines Notebooks als Handgepäck sollte darauf geachtet werden, dass es möglichst versteckt getragen wird, um es vor Diebstahl zu schützen. Bei der Arbeit in öffentlichen Verkehrsmitteln ist es wichtig, ausreichenden Sichtschutz zu haben, um zu verhindern, dass unbefugte Personen mitschauen können. Es sollten keine personenbezogenen oder sensible Daten verarbeitet werden. Um Daten, die auf Reisen erfasst wurden, und erstellte Verarbeitungsergebnisse auf zentrale Systeme oder mobile Datenträger zu sichern, ist es wichtig, regelmäßig eine sichere Verbindung zu verwenden. Sicherungsdatenträger sollten verschlüsselt und getrennt vom Notebook aufbewahrt werden. Bei Auslandsreisen sollten auch die speziellen Risiken, Vorkehrungen und Vorschriften beachtet werden. Es ist wichtig, den örtlichen Vorschriften zu folgen und darauf zu achten, dass Daten und Geräte auch in anderen Ländern sicher sind. Es ist ratsam, entsprechende Vorkehrungen zu treffen, um Daten und Geräte auf Reisen zu schützen, da sie potenzielle Sicherheitslücken darstellen können. Eine sorgfältige Planung und die Umsetzung von Schutzmaßnahmen können helfen, die Sicherheit von Daten und Geräten zu gewährleisten.

Darüber hinaus sind folgende Vorsichtsmaßnahmen zu beachten:

- Die Festplatten portabler Geräte (Notebooks) sind mit Bitlocker zu verschlüsseln.
- Jedes mobile Gerät ist mit einem sicheren Passwort nach den Vorgaben einer Richtlinie oder durch ein anderes sicheres und zugelassenes Verfahren zu sichern.
- In Privaträumen ist ein unbefugter Zugang auszuschließen.
- Ein Zugriff durch unbefugte Personen oder eine Überlassung des Notebooks an Dritte zur Nutzung, auch an Familienangehörige, ist unzulässig.
- Werden Notebooks von wechselnden Benutzern oder in unsicheren bzw. unbekannten Umgebungen eingesetzt, sind sie einem regelmäßigen Sicherheitscheck zu unterziehen.
- In öffentlichen Räumen, z. B. in Verkehrsmitteln etc., sind an den Notebooks Blickschutzfilter zu verwenden, ansonsten ist eine Verarbeitung von personenbezogenen oder sonstigen sensiblen Daten unzulässig.
- Mobile Geräte dürfen nicht unbeaufsichtigt sein und müssen zugriffsicher verwahrt werden.
- Zum Anschluss an unternehmensfremde Rechner dürfen nur mobile Geräte verwendet werden, die keine personenbezogenen oder sonstige vertrauliche Daten enthalten.
- Nach einem Anschluss an Fremdrechner müssen die mobilen Geräte auf Freiheit von Viren und sonstiger Schadsoftware geprüft werden.
- Arbeitsplatzrechner (Desktops, Notebooks, Handhelds, usw.) sowie Peripheriegeräte sind einzuschließen, wenn sie nicht unter Aufsicht sind.
- Bei Gesprächen und Besprechungen über vertrauliche Sachverhalte ist darauf zu achten, dass diese Gespräche nicht von unbefugten Personen belauscht werden können.
- Das Speichern oder Verarbeiten von internen und vertraulichen Informationen auf fremden Systemen ist unzulässig.
- Interne und vertrauliche Informationen dürfen nur auf Druckern ausgedruckt werden, bei denen die Ausgabe geeignet geschützt ist und sind umgehend vom Drucker abzuholen. Drucker und Kopierer mit umfangreichen Speicherfunktionen sollten für einen Ausdruck von vertraulichen Informationen vermieden werden.

4.3 Einsatz und Freigabe von Software

Bevor personenbezogene oder vertrauliche Daten erhoben, verarbeitet oder genutzt werden, müssen die dafür benötigten Systeme und Programme (Hard- und Software) einer erfolgreichen Prüfung und Freigabe unterzogen werden. Auch bei der Einführung von Standardsoftware, der Installation von Updates oder sonstigen Änderungen an Programmen oder Verfahren gilt dieser Grundsatz. Der Umfang der Prüfung und Freigabe ist in der Verfahrensdokumentation festgelegt und muss im Einzelfall bestimmt werden. Wenn neue Verfahren oder Anwendungen zum Einsatz kommen sollen, muss schriftlich bei der IT-Leitung um Genehmigung gebeten werden.

4.4 Einsatz privater Hard -und Software und privater Nutzung von betrieblichen Geräten

4.4.1 Private Geräte

Die Nutzung von privater Hard- und Software wie Notebooks, USB-Sticks, Speicherkarten und mobilen Laufwerken zu betrieblichen Zwecken sowie die Verwendung privater Datenträger, wie Disketten, CDs und Speichersticks an Firmen-PCs ist gemäß den betrieblichen Richtlinien untersagt.

4.4.2 Nutzung betrieblicher Geräte für private Zwecke

Es ist untersagt, betriebliche Hard- und Software für private Zwecke zu nutzen sowie betriebliche mobile Datenträger an privaten Geräten zu verwenden. Gleiches gilt für die betriebliche Nutzung von firmeneigenen mobilen Datenträgern an privaten Geräten und deren Überlassung an betriebsfremde Personen, einschließlich Familienangehörigen. Kopien von Programmen dürfen ausschließlich für betriebliche Zwecke erstellt werden, und nur in dem Umfang, der im Rahmen der Lizenzbedingungen zulässig und aus betrieblichen Gründen erforderlich ist. Sobald die Kopien nicht mehr benötigt werden, sind sie zu löschen oder zu vernichten. Die Erstellung von Kopien von Daten ist ebenfalls ausschließlich für betriebliche Zwecke und nur in Absprache mit dem Informationseigentümer zulässig, abhängig von ihrem Vertraulichkeitsgrad.

4.5 Verwaltung und Administration von Datenverarbeitung - Prozesse

4.5.1 Administrationsrechte

Administratoren sind nur dann mit privilegierten Rechten auszustatten, wenn es zwingend erforderlich ist, um ihre administrativen Aufgaben auszuführen. Für Aufgaben, die ohne diese Rechte ausgeführt werden können, sollten Standard-Accounts verwendet werden. Der Zugriff des Administrators auf betriebliche Inhaltsdaten ist ausschließlich nach Anordnung des zuständigen Bereichsverantwortlichen gestattet. Wenn es um private Inhalte geht, wie z. B. private E-Mails, darf der Administrator nur mit Einwilligung des Betroffenen darauf zugreifen. Diese Einwilligung sollte vorzugsweise im Vier-Augen-Prinzip oder in Anwesenheit des Betroffenen erfolgen. Beachten Sie, dass diese Regelung nicht für Zugriffe gilt, die im Verdacht auf eine Straftat im Beschäftigungsverhältnis oder zur Abwehr von Gefahren (im Falle von Gefahr im Verzug) erforderlich sind.

4.5.2 Überwachung von Schnittstellen und Zugänge

Schnittstellen zu externen Geräten, wie WLAN- oder USB-Schnittstellen sowie externe Laufwerke, wie CD- oder DVD-Laufwerke werden deaktiviert, wenn sie nicht benötigt werden. Wenn diese Schnittstellen für die Erfüllung von Aufgaben erforderlich sind, werden sie überwacht, um sicherzustellen, dass nur autorisierte und genehmigte Geräte

angeschlossen werden. Nicht benötigte Netzwerkzugänge werden ebenfalls deaktiviert oder in geeigneter Weise überwacht, um den Anschluss unbefugter Geräte frühzeitig zu erkennen und zu verhindern. Jeder Zugang mit unbefugten Geräten wird protokolliert und automatisch unterbunden. Wir sind stolz darauf, dass wir auf diese Weise die Sicherheit unserer IT-Systeme und unserer Daten gewährleisten.

4.6 Verwaltung und Bewertung von Unternehmenswerten

Die Sicherheit von Informationswerten wurde umfassend gewährleistet. Eine detaillierte Inventarliste wurde erstellt, die sämtliche relevanten Informationswerte enthält. Jeder dieser Werte wurde einem Informationsverantwortlichen zugewiesen, der anhand eines sorgfältig entwickelten Klassifizierungsschemas den Schutzbedarf ermittelt hat. Dadurch ist sichergestellt, dass alle Informationswerte angemessen geschützt sind und die Schutzziele der Informationssicherheit, wie Vertraulichkeit, Integrität und Verfügbarkeit, vollständig berücksichtigt wurden.

Um sicherzustellen, dass die Schutzmaßnahmen kontinuierlich aktualisiert und verbessert werden, wird die Inventarliste regelmäßig von den Informationsverantwortlichen überprüft. Diese Überprüfung erfolgt mindestens einmal jährlich, um sicherzustellen, dass die Klassifizierung der Informationswerte und die angewandten Schutzmaßnahmen nach wie vor relevant und angemessen sind.

Durch die konsequente Umsetzung dieses Inventarisierungs- und Klassifizierungsprozesses wurde gewährleistet, dass alle erforderlichen Schutzmaßnahmen identifiziert und implementiert wurden, um die Sicherheit aller Informationen und des organisatorischen Know-hows zu gewährleisten. Die Organisation kann somit sicher sein, dass ihre Informationswerte angemessen geschützt sind und potenzielle Risiken effektiv minimiert werden.

4.7 Lieferanten

Bei der Zusammenarbeit mit Kooperationspartnern und Auftragnehmern ist es von großer Bedeutung, dass ein angemessenes Sicherheitsniveau für Informationen aufrechterhalten wird. Hierbei gelten unsere strengen Regeln für Informationssicherheit, insbesondere wenn es um Daten unserer Kunden geht, die entsprechend ihrem Schutzbedarf behandelt werden müssen. Wir bewerten die Auftragnehmer anhand ihres Schutzbedarfs und ordnen sie einer Schutzstufe zu. Um die Einhaltung der Informationssicherheit zu gewährleisten, müssen wir mit Auftragnehmern der Schutzstufen "hoch" und "sehr hoch" mindestens eine Geheimhaltungsvereinbarung sowie eine Verpflichtung auf Informationssicherheit abschließen. Eine verbindliche Regelung hierzu enthält das Dokument "3.0 - 41 Informationssicherheitsleitlinie". Die Einhaltung dieser Regeln wird regelmäßig überprüft und dokumentiert.

4.8 Datenschutz

Im Rahmen unserer Geschäftstätigkeiten erlangen wir personenbezogene Daten von den Kontakten unserer Kunden und Lieferanten. Wir haben die Vorschriften zum Umgang mit personenbezogenen Daten und zum Datenschutz in einem Datenschutz-Handbuch dokumentiert. Die Einhaltung und Umsetzung der Anforderungen gemäß der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) wird durch unseren externen Datenschutzbeauftragten, Kutzschbach, überwacht. Anfragen zum Datenschutz werden ausschließlich durch den externen Datenschutzbeauftragten beantwortet.

4.9 Schulung Mitarbeiter

Es besteht ein potenzielles Risiko, wenn Mitarbeiter nicht über die Anforderungen und Risiken der Informationssicherheit informiert sind und demzufolge sich fehl verhalten. Es ist daher von wesentlicher Bedeutung, dass Informationssicherheit als integraler Bestandteil innerhalb des Unternehmens verstanden und praktiziert wird.

Die Mitarbeiter werden gemäß unserem Schulungskonzept zu den geplanten Schulungsmaßnahmen eingeladen. Die Teilnahme an den Schulungen ist grundsätzlich verpflichtend. Die Geschäftsleitung kann in besonderen Fällen jedoch Ausnahmen für einzelne Mitarbeiter zulassen.

5. NUTZUNG UND UMGANG VON INFORMATIONSTECHNOLOGIEN

5.1 IT-Sicherheit

5.1.1 Allgemeine Grundsätze

Es ist zu beachten, dass bei der Nutzung von IT-Systemen personenbezogene Daten und Geschäftsdaten ausschließlich in den dafür vorgesehenen Laufwerken, Verzeichnissen und Ordnerstrukturen gespeichert werden dürfen. Der Mitarbeiter ist lediglich befugt, innerhalb dieser Struktur Unterordner anzulegen. Eine alleinige Speicherung von Originaldaten auf lokalen Datenträgern, wie mobile Festplatten oder Speichersticks ist nicht gestattet. Es ist notwendig, gegebenenfalls Kopien anzufertigen.

Des Weiteren ist es geboten, nicht mehr benötigte Dateien und E-Mails regelmäßig zu löschen.

5.1.2 Verbindung von externen IT-Systemen

Gemäß den IT-Sicherheitsrichtlinien dürfen Verbindungen von vernetzten PCs zu externen Systemen und Netzen ausschließlich über die von den Verantwortlichen freigegebenen und kontrollierten Verbindungswege hergestellt werden. Dies gilt insbesondere für den Zugriff auf das Internet, bei dem WLAN-Verbindungen (z. B. in Hotels, auf Flughäfen,

Bahnhöfen oder in Zügen) im erforderlichen Umfang zulässig sind, sofern die dafür vorgesehenen Schutzmechanismen vorhanden, aktuell und funktionsfähig sind.

Es ist von größter Wichtigkeit, dass die Sicherheitsmaßnahmen gegen unautorisierte Zugriffe auf die IT-Infrastruktur des Unternehmens stets auf dem neuesten Stand sind. Hierbei müssen insbesondere die durch die IT-Abteilung definierten und kontrollierten Verbindungswege genutzt werden, um das Risiko von Sicherheitsverletzungen zu minimieren.

Die Nutzung von öffentlichen WLAN-Verbindungen stellt ein erhöhtes Risiko dar, da hierbei unverschlüsselte Verbindungen oder Schwachstellen in der Netzwerksicherheit ausgenutzt werden können. Deshalb müssen die vorgesehenen Schutzmechanismen wie beispielsweise Firewall- und Virenscan-Programme stets aktuell und funktionsfähig sein, um die Sicherheit der IT-Infrastruktur zu gewährleisten.

Eine Nichteinhaltung der oben genannten IT-Sicherheitsrichtlinien kann schwerwiegende Folgen haben und rechtliche Konsequenzen nach sich ziehen. Daher ist es unbedingt erforderlich, dass sich jeder Mitarbeiter an diese Vorgaben hält und bei Fragen oder Problemen umgehend die IT-Abteilung informiert.

5.1.3 Fremdkommunikationsressourcen

Grundsätzlich dürfen Fremdrechner, das heißt Rechner von Dritten, die nicht der Kontrolle der firmeneigenen Verantwortlichen unterstehen, nicht ohne deren Genehmigung an das Firmennetzwerk angeschlossen werden. Eine solche Genehmigung ist durch die zuständige Abteilung einzuholen, falls erforderlich. Sofern es erforderlich ist, Fremd- oder Kooperationsunternehmen einen Zugang zu personenbezogenen oder vertraulichen Daten zu gewähren, darf dies nur auf Anordnung des Fachbereichsverantwortlichen oder des Informationseigentümers und nur im zwingend erforderlichen Umfang erfolgen. Der Zugang muss über sichere Verbindungen mit zuverlässiger Identifizierung und Authentifizierung der Benutzer und erst nach Freigabe durch den IT-Verantwortlichen oder einen von ihm befugten Mitarbeiter erfolgen. Die Sicherheitsmaßnahmen sind abhängig vom Schutzbedarf der Daten und den mit dem Zugang verbundenen Risiken festzulegen.

Servicepartnern darf nur über definierte sichere Zugänge und Pfade mit sicherer und zuverlässiger Authentifizierung ein Zugang gewährt werden. Wenn Fremdunternehmen oder andere Personen Zugang zu Sicherheitsbereichen oder personenbezogenen oder vertraulichen Daten oder Informationen benötigen, müssen diese Personen während ihrer Tätigkeit in geeigneter Weise überwacht werden. Die Einzelheiten und Sicherheitsanforderungen sind in den entsprechenden Verträgen und gegebenenfalls in Vertraulichkeitsvereinbarungen zu regeln. Die zu vergebenden Berechtigungen sind unter Berücksichtigung des Schutzbedarfs der Daten und Informationen abzuwägen und nur im

geringstmöglichen Umfang zu erteilen. Soweit möglich, müssen die Aktivitäten dieser Stellen revisionssicher protokolliert und überprüft werden.

5.1.4 Wechseldatenträger

Zum Schutz personenbezogener und sonstiger vertraulicher Unternehmensdaten bei der Verwendung mobiler Datenträger sind folgende Vorschriften zu beachten:

- Auf mobilen Datenträgern wie mobilen Plattenlaufwerken, USB-Sticks, Speicherkarten und CDs/DVDs dürfen ausschließlich Kopien von Firmendaten gespeichert werden, um Datenverluste zu vermeiden. Sofern personenbezogene oder anderweitig vertrauliche Daten gespeichert werden, sind diese zu verschlüsseln.
- Es ist ausschließlich gestattet, mobile Datenträger zu geschäftlichen Zwecken zu verwenden, die von der IT-Abteilung freigegeben oder bereitgestellt wurden. Die Vergabe und Vernichtung von mobilen Datenträgern sind revisionsfähig zu dokumentieren.
- Mobile Datenträger müssen regelmäßig auf Virenfreiheit überprüft werden, insbesondere nach der Anschließung an fremde Systeme, der Speicherung von Daten aus externen Quellen oder vor dem Transfer von Fremddaten in firmeneigene Systeme.
- Eine Weitergabe von Daten und das Kopieren auf fremde Datenträger ist nur im Rahmen der Vertraulichkeitsrichtlinien gestattet und nur so weit, wie es für die Erfüllung betrieblicher Aufgaben unbedingt erforderlich ist.
- Personenbezogene oder andere vertrauliche Daten dürfen nicht unverschlüsselt auf Wechseldatenträgern gespeichert werden.
- Mobile Datenträger müssen stets zugriffssicher verwahrt und dürfen nicht unbeaufsichtigt sein.
- Zum Anschluss an unternehmensfremde Rechner dürfen nur mobile Datenträger verwendet werden, die keine personenbezogenen oder vertraulichen Daten enthalten. Diese mobilen Datenträger sollten möglichst über einen Schreibschutz verfügen und im schreibgeschützten Zustand verwendet werden.
- Nicht mehr benötigte Daten auf mobilen Datenträgern müssen unverzüglich sicher gelöscht werden.

5.1.5 Firewall und Viren-Schutz

Zusätzlich zu den zentralen Sicherheitsmaßnahmen werden alle Computer und Laptops durch eine lokal installierte Firewall und Internetsicherheitssoftware geschützt. Eine entsprechende Anleitung und Benutzerhinweise sind verfügbar. Dadurch sind die Geräte auch bei einem externen Zugang zum Internet angemessen geschützt. Um eine kontinuierliche Sicherheit der Geräte zu gewährleisten, ist es untersagt, Sicherheitssoftware zu installieren oder zu betreiben, die nicht von der IT-Abteilung freigegeben wurde. Die Konfiguration der Schutzsoftware darf nicht geändert werden und es ist strengstens untersagt, die Schutzsoftware zu deaktivieren oder zu deinstallieren.

Insbesondere darf die automatische Aktualisierung der Schutzsoftware nicht deaktiviert oder verändert werden, und die Geräte dürfen nur bei aktuellem Schutzstatus mit dem Internet verbunden werden.

Die Konfiguration der Firewall sowie deren Funktionsfähigkeit sind in angemessenen Abständen von der verantwortlichen Abteilung zu überprüfen.

5.1.6 Passwörter

Der Zugang zu Datenverarbeitungsverfahren ist ausschließlich über ein sicheres Anmeldeverfahren gestattet, welches speziell bei sensiblen Verfahren ausgestaltet sein muss, um Datum und Uhrzeit des letzten erfolgreichen oder erfolglosen Anmeldeversuchs anzuzeigen und erfolglose Anmeldeversuche zu protokollieren. Die Identifizierung und Authentifizierung der Benutzer erfolgen über ein persönliches Login, das jeder Mitarbeiterin und jedem Mitarbeiter zugewiesen ist, sowie über ein zusätzliches Passwort. Das Passwort stellt den Schlüssel zur Identifikation des Berechtigten dar und muss daher vertraulich behandelt werden. Um die Sicherheit des Passworts zu gewährleisten, müssen bestimmte Regeln beachtet werden, die in ausreichendem Maße automatisiert durchgesetzt werden müssen. Der Zugang ist nach drei bis fünf erfolglosen Anmeldeversuchen zu blockieren und darf erst nach einer zweifelsfreien Identifikation des Benutzers wieder freigegeben werden.

5.1.7 Unbefugte Kenntnisnahme von Unternehmenswerten

In Räumlichkeiten mit Publikumsverkehr müssen IT-Arbeitsplätze so angeordnet werden, dass Dritte keinen unmittelbaren Einblick auf die Bildschirme erhalten. Bei Bedarf sind die Monitore mit Sichtschutzfolien zu versehen, um unbefugte Einsichtnahmen zu verhindern. Drucker dürfen nur in gesicherten Bereichen aufgestellt werden, die für unbefugte Personen unzugänglich sind. Nach dem Druckvorgang müssen Ausdrucke unverzüglich aus dem Drucker entfernt werden. Wenn möglich, insbesondere bei vertraulichen Angelegenheiten, sollten vertrauliche Druckfunktionen verwendet werden. Bei Verlassen des Arbeitsplatzes muss sich der Benutzer am System abmelden oder die Tastatur/Bildschirmsperre (passwortgeschützter Bildschirmschoner) aktivieren. Unabhängig davon muss die Sperre automatisch nach einer Zeitspanne von fünf bis zehn Minuten ohne Benutzereingabe wirksam werden. Datenträger, Ausdrucke oder andere Unterlagen mit vertraulichem oder streng vertraulichem Inhalt müssen grundsätzlich bei Verlassen des Arbeitsplatzes unter Verschluss gehalten werden. Bei Arbeitsende müssen Endgeräte wie PCs oder Drucker ausgeschaltet werden. Notebooks, die nicht durch ein Kabelschloss gesichert sind, müssen bei Arbeitsende eingeschlossen werden. Sofern keine anderen Vorschriften entgegenstehen, müssen abschließbare Einzelbüros beim Verlassen verschlossen werden.

5.1.8 Identitätsfeststellung von Mitarbeitern

Die Ausgabe von Identifikationsmitteln, wie Schlüssel, Fingerprint obliegt der Personalabteilung. Die IT-Abteilung ist für die Ausgabe, Verwaltung, Rücknahme und Vernichtung von Identifikationsmitteln in Form von Soft-, Hardware-Token zur Gewährleistung des Zugangs zur Unternehmensumgebung zuständig. Die zeitliche Begrenzung von Identifikationsmitteln richtet sich nach den jeweiligen Zutrittsbereichen. Sollten Identifikationsmittel verloren gehen, ist dies unverzüglich sowohl der Personalabteilung als auch der IT-Abteilung mitzuteilen.

5.1.9 Besucher

Gemäß den geltenden Bestimmungen werden Besucher, die eine bestimmte Stelle oder Person innerhalb des Unternehmens besuchen, in einem Besucherinformationssystem erfasst. Hierbei ist der Name des Besuchers sowie der Beginn und das Ende der Besuchszeit zu dokumentieren. Die Überwachung von Besuchern innerhalb des Unternehmens ist erforderlich, um die Sicherheit zu gewährleisten. Zu diesem Zweck sind die Besucher innerhalb der Sicherheitsbereiche zu beaufsichtigen. Um die Sicherheit der Unternehmensbereiche weiterhin zu gewährleisten, dürfen Besucher innerhalb der Sicherheitsbereiche keine Fotohandys oder andere Bild- oder Tonaufzeichnungsgeräte mit sich führen. Die spezifischen Bestimmungen zur Umsetzung dieser Maßnahmen obliegen dem jeweils zuständigen Fachbereichsverantwortlichen des entsprechenden Sicherheitsbereichs.

5.2 Sicherheitsvorfälle

5.2.1 Diebstahl und Verlust vom Arbeitgeber überlassenen Geräte

Gemäß der arbeitsvertraglichen Vereinbarung ist der Mitarbeiter zur Sicherung der ihm anvertrauten Geräte gegen Diebstahl verpflichtet. Sollte es zu einem Diebstahl oder sonstigen Verlust von mobilen Geräten oder Datenträgern kommen, obliegt es dem Mitarbeiter, unverzüglich den Vorgesetzten und die zuständige IT-Abteilung darüber zu informieren. Diese haben daraufhin die gebotenen Maßnahmen einzuleiten.

5.2.2 Verhalten bei Systemausfällen und Störungen

Gemäß der Definition sind Sicherheitsvorfälle als Vorfälle zu betrachten, bei denen der Verlust oder das Risiko des Verlusts oder der Zerstörung von Daten oder ihrer Vertraulichkeit, Integrität, Authentizität und Revisionsfähigkeit gegeben ist. Diese Vorfälle müssen dem Informationssicherheitsbeauftragten gemeldet werden.

Im Falle eines Sicherheitsvorfalls oder eines entsprechenden Verdachts sowie bei sonstigen Störungen ist wie folgt vorzugehen:

- Jeglicher Ausfall oder Störungen von IT-Systemen sind unverzüglich dem IT-Leiter/IT-Sicherheitsbeauftragten zu melden, unabhängig von der Art und Schwere des Vorfalls und der Anzahl der betroffenen Systeme/Arbeitsplätze. Der IT-Leiter/IT-Sicherheitsbeauftragte entscheidet je nach Art des Vorfalls über die weitere Vorgehensweise und über die zu benachrichtigenden bzw. einzuschaltenden Stellen, z. B. fachverantwortliche Stellen, Personalabteilung, Datenschutzbeauftragter etc.
- Jeder Vorfall ist nach Art und Ausmaß, betroffenen Verfahren, Daten und Stellen zu dokumentieren.
- Die Art der Behebung des Vorfalls sowie die eingeleiteten rechtlichen, organisatorischen und technischen Maßnahmen sind zu dokumentieren.
- Der durch den Vorfall entstandene Schaden ist zu bewerten. Dabei sind auch immaterielle Schäden zu berücksichtigen, z. B. Auswirkungen auf Kunden, Beschäftigte, Öffentlichkeit etc., und es ist ein Schadensbericht zu erstellen.
- Die Ursachen des Vorfalls sind zu analysieren und es sind nach Möglichkeit Maßnahmen abzuleiten und einzurichten, um ähnliche Vorfälle in Zukunft zu vermeiden.
- Im Falle eines Verlusts der Vertraulichkeit der Daten sind eventuelle Informationspflichten der Betroffenen und der Datenschutzaufsichtsbehörde zu beachten.
- Die Mitarbeiter dürfen nicht versuchen, den Vorfall selbst aufzuklären oder etwas gegen den Verursacher zu unternehmen. Grundsätzlich ist dabei Folgendes zu beachten:
    - Laufende Programme sind zu beenden.
    - Neue Programme dürfen nicht mehr gestartet werden.
    - Es dürfen keine Daten oder E-Mails mehr versandt werden.
    - Systemhinweise und Systemmeldungen sind festzuhalten.

- Die Dokumentationen über Sicherheitsvorfälle sind regelmäßig statistisch aufzuarbeiten und nach Art, Umfang, Kosten, Risiko- und Gefahrenpotenzial der Vorfälle auszuwerten. Aus den Auswertungen sind unter dem Gesichtspunkt des Lernens aus Vorfällen Maßnahmen zur künftigen Vermeidung ähnlicher Vorfälle und zur Verbesserung der Informationssicherheit abzuleiten.

5.3 Sicherung und Backupmaßnahmen

5.3.1 Sicherung von zentralen Datenbeständen

Die zentrale Datensicherung erfolgt auf der Grundlage eines festgelegten Sicherungskonzepts auf vorgesehene Systeme und Datenträger.

5.3.2 Sicherung von lokalen Datenträgern

Daten auf lokalen Festplatten, z. B. von Arbeitsplatz-PCs oder auf sonstigen mobilen Datenträgern werden nicht gesichert und sind im Schadensfall verloren. Ungesicherte Laufwerke, z. B. lokale oder persönliche Laufwerke dürfen deshalb nicht als alleiniger Speicherort für geschäftskritische Daten verwendet werden.

5.3.3 Ausscheiden, Versetzung und Abwesenheit von Mitarbeitern

Jeder Mitarbeiter ist verpflichtet, vor seinem Ausscheiden, seiner Umsetzung bzw. Abwesenheit alle für das Unternehmen noch relevanten und aufbewahrungspflichtigen Dokumente und Daten zu übergeben und private bzw. nicht mehr erforderliche Vorgänge zu löschen. Die Übergabe der Daten und Dokumente ist vom Vorgesetzten und die Löschung der privaten Vorgänge vom Betroffenen zu bestätigen.

5.4 Verwaltung von Benutzerkonten

Gemäß den vorliegenden Bestimmungen dürfen die Benutzer nur auf diejenigen Programme, Laufwerke, Ordner und Dateien zugreifen, die für die Erfüllung ihrer betrieblichen Aufgaben notwendig sind. Dies wird durch individuelle Rechte und Berechtigungen für die eingesetzten Systeme und Anwendungen gewährleistet. Die Vergabe von Berechtigungen muss restriktiv gehandhabt werden und darf nur im notwendigen Umfang erfolgen. Es ist den Mitarbeitern untersagt, sich außerhalb der für ihre Arbeitsaufgaben vorgesehenen Systeme und Datenbereiche zu bewegen, auch wenn dies aufgrund unzureichender Rechtevergabe oder technischer Mängel möglich ist. Sollte dies der Fall sein, ist der Vorgesetzte oder der IT-Leiter/IT-Sicherheitsbeauftragte zu informieren. Die Einrichtung von Benutzerkonten und Zugriffsrechten erfolgt durch die IT-Administration auf schriftliche Anforderung der Fachvorgesetzten. In dieser Anforderung müssen die freizugebenden Anwendungen und erforderlichen Rechte festgelegt werden. Jegliche Anforderungen zur Anlage oder Stilllegung von Benutzerkonten und zur Vergabe oder Entziehung von Benutzerrechten erfordern eine schriftliche Anforderung, um eine angemessene Dokumentation zu gewährleisten. Es ist den Mitarbeitern nicht gestattet, Administratorrechte zu besitzen, es sei denn, es gibt triftige Gründe dafür. Sollte dies erforderlich sein, dürfen Administrationsrechte nur im notwendigen Umfang für betriebliche Aufgaben eingesetzt werden. Sicherheitsrelevante Einstellungen oder Standardsystemeinstellungen dürfen nicht verändert werden.

Beim Ausscheiden des Mitarbeiters, bei Versetzungen oder bei einem Wechsel von Aufgaben und Zuständigkeiten ist unverzüglich die Löschung von nicht mehr benötigten Berechtigungen durch die jeweiligen Vorgesetzten zu veranlassen. Neue Zugriffsrechte müssen entsprechend dem neuen Aufgabengebiet beauftragt und eingerichtet werden. Zur Überprüfung der Rechtevergabe ist eine Kontrolle durch die Fachvorgesetzten in regelmäßigen Abständen, beispielsweise jährlich oder halbjährlich, vorzunehmen, um sicherzustellen, dass die eingerichteten Berechtigungen noch notwendig sind. Nicht mehr

erforderliche Berechtigungen sind zu löschen. Die Anmeldung am Firmennetzwerk von Externen ist nur mittels 2-Faktor-Authentifizierung gestattet.

5.5 Sicherheit gegen Schadprogramme

Zur Prävention von Schäden durch Schad- und Spionagesoftware sind bestimmte Vorgaben zu beachten. Eine Verbindung von vernetzten PCs zu externen Netzen außerhalb des Unternehmens ist nur im erforderlichen Umfang und nach sicherheitstechnischer Prüfung und Freigabe durch die IT-Administration zulässig, wobei die von der IT eingerichteten Schutzmaßnahmen vorhanden, aktuell und funktionsfähig sein müssen. Alarme der Virenscanner, Computeranomalien und Systemereignisse oder sonstige Auffälligkeiten, die auf die Aktivierung unbekannter Software hindeuten, sind unverzüglich der IT-Systemadministration zu melden. Eine eigenmächtige Veränderung von Sicherheitseinstellungen ist unzulässig. Bei Verdacht auf eine Vireninfektion sind bestimmte Schritte zu befolgen, und die IT-Administration ist umgehend zu verständigen. Es ist darauf zu achten, dass auch die Regeln zum Datenschutz bei der Nutzung von E-Mail und Internet beachtet werden.

5.6 Weitergabe, Löschung und Entsorgung von Geräten und Datenträgern

5.6.1 Weitergabe von elektronischen Datenträgern

Gemäß den vorgesehenen Verfahren und unter Beachtung der Befugnisse dürfen Datenträger ausschließlich an autorisierte Personen weitergegeben werden. Jegliche Abweichungen hiervon bedürfen der vorherigen Genehmigung durch die zuständige fachverantwortliche Stelle. Soweit es sich um personenbezogene oder andere vertrauliche Daten handelt, hat der Empfänger diese Daten zu quittieren. Beim Versand von Datenträgern ist ein zuverlässiger Versandweg zu wählen, der eine lückenlose Nachweisbarkeit des Versands und des Empfangs der Datenträger gewährleistet. Vor dem Versand von personenbezogenen oder anderen vertraulichen Daten sind diese Daten verschlüsselt zu übermitteln.

5.6.2 Löschung und Entsorgung von Datenträgern

- **Löschung**

Es besteht die Verpflichtung, sämtliche personenbezogenen und sonstigen Unternehmensdaten unverzüglich zu löschen, sobald sie für die Erfüllung der betreffenden Aufgabe nicht mehr benötigt werden und keine Aufbewahrungsfristen anwendbar sind oder solche Fristen bereits abgelaufen sind. Die Anordnung der Löschung obliegt der fachverantwortlichen Stelle und muss schriftlich erfolgen, unter Berücksichtigung gegebenenfalls bestehender Aufbewahrungsfristen oder des Aufbewahrungsinteresses des

Unternehmens oder betroffener Personen. Für die Löschung von elektronischen Datenträgern sind sichere Löschverfahren wie Löschprogramme anzuwenden, die durch mehrfaches Überschreiben der gespeicherten Daten eine zuverlässige und nicht wiederherstellbare Löschung gewährleisten.

- **Vernichtung**

Bei der Vernichtung und Entsorgung von Datenträgern müssen alle erforderlichen Maßnahmen getroffen werden, um sicherzustellen, dass keine personenbezogenen oder anderweitig vertraulichen Daten in unbefugte Hände geraten. Dabei sind die geltenden Datenschutzbestimmungen zu beachten. Dienstleistungsunternehmen, die mit der Vernichtung von Datenträgern beauftragt werden, sind verpflichtet, die Vorschriften zur Datenverarbeitung im Auftrag einzuhalten. Elektronische Datenträger, die entsorgt werden sollen, müssen vom Benutzer an der von der IT eingerichteten Sammelstelle abgegeben werden. Dort werden sie gesammelt, aufbereitet oder vernichtet bzw. in geeigneter Weise entsorgt. Sofern die Datenträger personenbezogene Daten oder Daten enthalten, die gemäß den Vertraulichkeitsrichtlinien als vertraulich einzustufen sind, müssen diese Datenträger vor ihrer Weitergabe zur Vernichtung mit einem Löschprogramm entsprechend dem aktuellen Stand der Technik sicher gelöscht werden. Ist ein Datenträger aufgrund eines Defekts nicht mehr ansprechbar, ist er zu vernichten. In Gewährleistungsfällen oder anderen besonderen Umständen kann der IT-Sicherheitsverantwortliche je nach Einzelfall (z. B. Art des Datenträgers, Art und Sensibilität der gespeicherten Daten, Garantiefall oder Reparaturtausch) unter Berücksichtigung der Sicherheitsanforderungen eine abweichende Entscheidung treffen. Handelt es sich bei einem Datenträger um besonders sensible oder anderweitig besonders vertrauliche Daten (z. B. Personaldaten) und ist eine sichere Löschung nicht möglich, so ist der Datenträger ausnahmslos zu vernichten.

- **Entsorgung**

Aufgrund der Tatsache, dass vertrauliche Informationen auch auf Papier vorliegen können, ist eine sorgfältige Sammlung von Altpapier sowie eine zuverlässige Entsorgung mit einer Bestätigung der datenschutzgerechten Vernichtung erforderlich. Die Vorgaben für die Vernichtung von Papier sind in der Norm DIN 66399 geregelt. Für als geheim einzustufendes Schriftgut ist nach dieser Norm die Vernichtung nach Schutzklasse 2 und Sicherheitsstufe 4 verpflichtend. Bei der Entsorgung von Papier ist darauf zu achten, dass diese Anforderungen eingehalten werden und dass das Entsorgungsunternehmen schriftlich bestätigt, dass eine datenschutzgerechte Vernichtung erfolgt ist.

6. REVISION

Gemäß dieser Richtlinie ist eine regelmäßige Überprüfung auf Aktualität, Vollständigkeit und Konformität zu den bestehenden rechtlichen, technischen und organisatorischen Rahmenbedingungen vorzunehmen. Diese Überprüfung ist im Abstand von jeweils zwölf Monaten durchzuführen und gegebenenfalls sind Ergänzungen oder Aktualisierungen vorzunehmen.