SAP GLOBAL SECURITY (SGS)

GLOBAL SECURITY POLICY

Versionsnummer: 1.3
Datum des Inkrafttretens: 6. April 2020
Dokumentklassifikation: INTERN | ***Genehmigt für die Verteilung an externe Parteien im Rahmen einer Geheimhaltungsvereinbarung (NDA) oder einer anderen geeigneten Vertraulichkeitsvereinbarung.***

THE BEST RUN SAP®

DECKBLATT

Ziel	Ziel dieser Policy ist die Definition allgemeiner Anforderungen, um: • Die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Assets zu wahren. • Alle Assets vor Bedrohungen – ob intern oder extern, absichtlich oder versehentlich – zu schützen, basierend auf einer Beurteilung der Risiken für das Unternehmen. • Sicherzustellen, dass gesetzliche, behördliche, betriebliche und vertragliche Anforderungen erfüllt werden.
Grundlage	
Warum – Vorteile und Strategieabstimmung	Die Verantwortung für die Sicherheit liegt zwar letztlich beim SAP-Vorstand, erstreckt sich aber auf alle Personen, die bei SAP oder deren verbundenen Unternehmen tätig sind. Eine entsprechende aktuelle globale Sicherheitsrichtlinie regelt die unternehmensweiten Anforderungen für den Schutz aller Mitarbeiter und deren Arbeit sowie der Informationen, die Kunden SAP anvertrauen.
Risiko für SAP bei Nichteinhaltung	Verstöße gegen Richtlinien führen zu einem erhöhten Risiko für SAP im Hinblick auf finanzielle Schäden, Schädigung des Ansehens, rechtliche Ansprüche, Verlust von Kunden oder von Chancen auf Vertragsabschlüsse. Die Nichterfüllung gesetzlicher Auflagen (Finanz- und/oder Sicherheitsprüfung) kann die Erteilung von Sicherheitszertifizierungen oder -nachweisen verhindern oder deren Verlust zur Folge haben, was wiederum den Verlust von Kunden oder von Chancen auf Vertragsabschlüsse nach sich ziehen kann.
Geltungsbereich	
Primäre Zielgruppe der Richtlinie	Diese Policy gilt für alle Unternehmen innerhalb von SAP, alle SAP-Mitarbeiter, alle externen Parteien, denen Zugriff auf Informationen von SAP erteilt worden ist, sowie für alle Informationen und Assets, die Eigentum von SAP sind oder von SAP verwaltet werden.
Indirekt betroffene Bereiche	Keine
Vertraulichkeit	Intern
Durchsetzung	Verletzungen dieser Policy können Disziplinarmaßnahmen gemäß dem vor Ort geltenden Arbeitsrecht bis hin zur Kündigung zur Folge haben.
Verantwortung	
Verantwortlich für die Richtlinie	Chief Security Officer, SAP
Vorstandsbereich	Office of the Co-CEOs
Prüfung durch	Diese Version 1.3, die Version 1.2 ersetzt, wurde am 31. März 2020 von Daniel Fryer, Head of Security Policy, Standards and Risk Management, geprüft und enthält eine kleinere inhaltliche Änderung. Version 1.2 wurde am 30. Mai 2019 von Tim McKnight, SAP Chief Security Officer, geprüft.
Genehmigt von	Diese Version 1.3, die Version 1.2 ersetzt, enthält eine kleinere inhaltliche Änderung und wurde am 31. März 2020 von Daniel Fryer, Head of Security Policy, Standards and Risk Management, genehmigt. Version 1.2 wurde am 30. Mai 2019 von Tim McKnight, SAP Chief Security Officer, genehmigt.
Dokumentinformationen	
URL des Masterdokuments	Dies ist die offiziell veröffentlichte Version.
Datum der Veröffentlichung	6. April 2020

DOKUMENTBEZEICHNUNG

Dokumentumfang	SAP Global
Verantwortlich für das Dokument	Chief Security Officer, SAP
Überprüfungs-turnus	Jährlich
Änderungs-verzeichnis	Das vollständige Änderungsverzeichnis kann unter folgender Adresse angefordert werden: SAP_Security_Policy@exchange.sap.corp.
Versionsnummer	1.3
Datum des Inkrafttretens	6. April 2020
Status	Veröffentlicht

INHALTSVERZEICHNIS

1 EINFÜHRUNG

SAP verpflichtet sich dazu, eine sichere Umgebung für unsere Mitarbeiter, unsere Informationen, unsere Assets und die Informationen, die uns von unseren Kunden und Partnern anvertraut werden, sicherzustellen. SAP setzt auf Branchenstandards und einen risikobasierten Ansatz zur Umsetzung einer Reihe von umfassenden und dokumentierten Sicherheitskontrollen, um unseren Sicherheitsstatus aufrechtzuerhalten. Dadurch werden wir auch in Zukunft das Sicherheitsniveau bieten, das unsere Kunden gewohnt sind, und den Ruf von SAP als vertrauenswürdiger und sicherer Geschäftspartner festigen.

2 INHALTE UND ZIELE

Zweck der **SAP Global Security Policy** (nachfolgend als „diese Policy“ bezeichnet) ist es, Governance und Struktur für Informationssicherheit auf angemessenem und effektivem Niveau innerhalb von SAP und ihren verbundenen Unternehmen zu bieten. Die Policy legt die strategischen Ziele fest, deren Aufrechterhaltung SAP anstrebt, und steht im Einklang mit der übergeordneten Unternehmensstrategie und -vision von SAP.

Ziel dieser Policy ist die Definition allgemeiner Anforderungen, um:

- Die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Assets zu wahren.
- Alle Assets vor Bedrohungen – ob intern oder extern, absichtlich oder versehentlich – zu schützen, basierend auf einer Beurteilung der Risiken für das Unternehmen.
- Sicherzustellen, dass gesetzliche, behördliche, betriebliche und vertragliche Anforderungen erfüllt werden.

3 GELTUNGSBEREICH

Diese Policy gilt für alle Unternehmen innerhalb von SAP, alle SAP-Mitarbeiter, alle externen Parteien, denen Zugriff auf Informationen von SAP erteilt worden ist, sowie für alle Informationen und Assets, die Eigentum von SAP sind oder von SAP verwaltet werden.

4 ÜBERPRÜFUNG, AKTUALISIERUNG UND PFLEGE

Diese Policy ist ein fortzuschreibendes Dokument. Es kann zum Schutz von SAP nach Bedarf abgeändert werden, wenn neue Bedrohungen und Schwachstellen erkannt werden oder sich das Risikoprofil des Unternehmens wandelt.

Die Policy muss einmal jährlich überprüft werden, im Falle wesentlicher Änderungen auch früher. Bei der Überprüfung sollten Verbesserungspotenziale ermittelt werden, um die Effektivität und Eignung dieser Policy weiterhin sicherzustellen.

SAP Global Security führt die alljährlichen Überarbeitungen durch und aktualisiert den Inhalt der Policy. Der Inhalt wird dann von den Mitgliedern des SAP Security Steering Committee genehmigt.

Kleinere inhaltliche und redaktionelle Änderungen sowie Klarstellungen und Formatierungsänderungen werden vom SAP Chief Security Officer genehmigt.

5 AUSNAHMEN

Ausnahmen von dieser Policy sind unter bestimmten Umständen möglich, wenn Kontrollen zur Eindämmung des damit verbundenen Risikos eingeführt werden.

Jeder Antrag muss über die SAP Global Security Policy Mailbox unter SAP_Security_Policy@exchange.sap.corp schriftlich eingereicht werden. Jedem Antrag ist ein Schreiben beizufügen, das die geschäftlichen Gründe für die Ausnahme, die möglichen Risiken und die vorgeschlagenen Maßnahmen zur Minderung dieser Risiken enthält.

SAP Global Security wird gemeinsam mit den entsprechenden Fachexperten die Ausnahmeanträge prüfen und den Antragstellern die Entscheidung mitteilen.

6 DURCHSETZUNG

Verletzungen dieser Policy können Disziplinarmaßnahmen gemäß dem vor Ort geltenden Arbeitsrecht bis hin zur Kündigung zur Folge haben.

7 BEGLEITDOKUMENTE

Diese Policy stützt sich auf verschiedene Policies, Standards, Verfahren und Richtlinien. In dieser Policy wird auf die folgenden Dokumente ausdrücklich Bezug genommen:

- SAP Global Information Classification and Handling Standard
- SAP Global Physical Security Standard
- SAP Global Risk Management Policy
- SAP IT Secure System Operation Standard
- SAP Mobile Device Security Procedure
- SAP Global Data Protection and Privacy Policy
- SAP Supplier Security Standard
- SAP Product Security Standard
- SAP Business Continuity and Operational Resilience Standard
- SAP Information Governance and Records Management Policy
- SAP Code of Business Conduct for Employees
- SAP Social Media Guidelines
- SAP Background Verification Process Guidelines

8 DEFINITIONEN

Assets (Vermögenswerte)	Etwas von materiellem oder immateriellem Wert; u. a. Personen, Informationen, Software, Hardware, Ausrüstung, Verfahren, Einrichtungen, ausgelagerte Dienstleistungen, geistiges Eigentum und Netzwerke
Asset-Verantwortlicher	Eine Person, die für das effektive Management eines Assets während dessen Lebensdauer verantwortlich ist.
Verfügbarkeit	Sicherstellen von zeitnahem und verlässlichem Zugriff auf und die Nutzung von Informationen durch dazu befugte Instanzen
Geschäftseinheit	Jede SAP-Instanz, die ggf. speziell für ihre Geschäftsprozesse zusätzliche Sicherheitsanforderungen benötigt.
Vertraulichkeit	Wahren von autorisierten Zugriffs- und Offenlegungsbeschränkungen, einschließlich Maßnahmen zum Schutz von Persönlichkeitsrechten und urheberrechtlich geschützten Informationen.
Datenspeichergerät	Jedes Gerät und jede Einheit, das bzw. die als Datenspeicher oder Datenträger fungiert. Dies umfasst u. a. interne und externe Festplattenlaufwerke, Backup-Medien (z. B. Tapes), Wechseldatenträger (z. B. Flash-Laufwerk oder CD) und Datenspeicher in mobilen Geräten.
Endbenutzergeräte	Client-Systeme, einschließlich: • Arbeitsstationen: feste Arbeitsplätze oder Desktop-Computer • Laptops: tragbare Computer • Mobile Geräte: Mobiltelefone, Personal Digital Assistants (PDAs), Tablets und andere tragbare Computer
Ephemeral Messaging (Flüchtiger Nachrichtenaustausch)	Anwendungen oder Services, bei denen übermittelte Nachrichten oder Audio-, Video- und andere Dateien sich nach einem bestimmten Zeitraum oder Ereignis (z. B. der Erkennung durch den Empfänger) automatisch und unwiederbringlich selbst löschen.
Externe Partei	Eine dritte Partei, der Zugriff auf Informationen oder Assets von SAP erteilt wird. Hierbei kann es sich u. a. um externe Mitarbeiter, Auftragnehmer, Berater, Unterauftragsverarbeiter, Kunden, Lieferanten und Partner handeln.

Informationen	Bedeutungsvolle und zweckmäßige Daten, die in unterschiedlicher Form, z. B. gedruckt, handschriftlich, mündlich oder elektronisch generiert oder gespeichert, vorliegen können.
Informationssicherheit	Die Kombination aus Prozessen und Kontrollmechanismen, die zum Schutz von Informationen vor verschiedenen Bedrohungen eingeführt wurden und deren Vertraulichkeit, Integrität und Verfügbarkeit gewährleisten
Integrität	Schutz von Systemen und Informationen vor unbefugten Veränderungen
Geistiges Eigentum	Patente, Urheberrechte, Geschäftsgeheimnisse, Marken und andere Rechte an geistigem oder gewerblichem Eigentum, die gesetzlich geschützt sind
IT-System	Technologiekomponente. Hierzu gehören u. a. Endbenutzergeräte (Arbeitsstationen, Laptops, mobile Geräte), Serversysteme, Netzwerkkomponenten, Software-Container und Virtualisierungsinfrastruktur.
IT System Owner	Eine Person, die für die IT-Systeme verantwortlich ist, die in der SAP-Infrastruktur betrieben werden.
Mobiles Gerät	Hierzu gehören Mobiltelefone, PDAs, Tablets und andere tragbare Geräte, auf denen ein Betriebssystem für mobile Endgeräte ausgeführt wird, das SAP-Informationen speichern und verarbeiten kann.
Partner	Gewinnorientiertes Unternehmen, mit dem SAP zusammenarbeitet
Personenbezogene Daten	Alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar gilt eine natürliche Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung (wie eines Namens, einer Kennnummer, Standortdaten, einer Online-Kennung) oder zu einem oder mehreren spezifischen Elementen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Principle of Least Privilege (Konzept der geringstmöglichen Rechte)	Das Prinzip, den Zugang auf die Mindeststufe zu beschränken, die notwendig ist, um eine normale Funktionsweise und die Ausführung einer Aufgabe zu ermöglichen.
Verarbeiten	Das Verändern und Übermitteln von Informationen sowie das Zugreifen darauf
Wechseldatenträger	Ein USB-/Flash-Laufwerk, eine CD, DVD, Diskette oder andere tragbare physische Speichergeräte, die zum Verschieben von Informationen von einem Gerät auf ein anderes eingesetzt werden können; auch als tragbare Medien bezeichnet
Risiko	Die Kombination der Eintrittswahrscheinlichkeit eines Ereignisses und seiner Folgen
SAP-Informationen	Informationen oder Daten, die für SAP von finanziellem oder rechtlichem Wert oder von Wert in Bezug auf ihre Wettbewerbsfähigkeit sind oder die SAP von externen Parteien wie Kunden oder Partnern anvertraut werden. Dies schließt auch Informationen oder Daten ein, die im Verlauf des Geschäftsbetriebs von SAP entstehen, in SAP-Systemen gespeichert oder verarbeitet, von anderen für SAP erstellt werden oder aufgrund von gesetzlichen, vertraglichen oder behördlichen Vorschriften des Schutzes durch SAP bedürfen.
SAP-Netzwerk	Das gesamte Netzwerk, das sich aus der Verbindung von mehreren lokalen Netzwerken über die WAN-Infrastruktur ergibt. Innerhalb des SAP-Netzwerks gibt es verschiedene Sicherheitszonen, die verschiedenen Sicherheits- und Risikostufen entsprechen.
Sicherheitskontrolle	Sicherheitsmaßnahme zur Risikominderung

Fremdsystem	Ein IT-System oder technisches Gerät, das von einem Partner, Kunden oder Lieferanten von SAP verwaltet wird oder dessen Eigentum ist. Die darauf installierte Software wird nicht von SAP IT gepflegt oder bereitgestellt.
Arbeitsstation	Ein fester Arbeitsplatz oder Desktop-Computer.

9 ORGANISATION DER INFORMATIONSSICHERHEIT

9.1 Rollen und Verantwortlichkeiten für Informationssicherheit

Die Sicherheitsaufgaben sind je nach Geschäftsanforderungen und in Abstimmung auf die Anforderungen dieser Policy zu verteilen. Die Mitglieder des Managements können Sicherheitsaufgaben an andere Personen delegieren. Sie bleiben jedoch dafür verantwortlich, dass die Aufgaben korrekt ausgeführt werden. Kollidierende Aufgaben und Zuständigkeitsbereiche müssen getrennt werden, um Möglichkeiten für Modifikationen oder missbräuchliche Nutzung von Assets zu reduzieren.

9.1.1 Geschäftsleitung

Für folgende Aspekte sind die Mitglieder der Geschäftsleitung verantwortlich:

- Sicherstellen, dass diese Policy sowie ihre Inhalte und Ziele auf die strategische Ausrichtung des Unternehmens abgestimmt sind
- Mit gutem Beispiel vorangehen und diese Policy unterstützen
- Engagement zeigen, um den Sicherheitsstatus des Unternehmens zu wahren, zu berücksichtigen und kontinuierlich zu verbessern
- Ausreichend Zeit, Ressourcen und Mittel für erforderliche Funktionen und Programme zur Verfügung stellen

9.1.2 Management

Für folgende Aspekte sind die Mitglieder des Managements verantwortlich:

- Sicherstellen, dass diese Policy und andere geltende Sicherheitsrichtlinien und Standards und in ihrem jeweiligen Verantwortungsbereich umgesetzt und durchgesetzt werden
- Sicherheitsrisiken nach der *SAP Global Risk Management Policy* und den geltenden Risikomanagementstandards identifizieren und behandeln
- Den Mitarbeitern in ihrem jeweiligen Verantwortungsbereich die geeigneten Räumlichkeiten, Systeme, Anwendungen und Datenzugriffsrechte zur Verfügung stellen
- Sicherstellen, dass die geeigneten Benutzerkonten geändert oder deaktiviert werden, wenn ein Mitarbeiter in den Verantwortungsbereich eines anderen Managementmitglieds wechselt oder das Unternehmen verlässt
- Dafür sorgen, dass die Mitarbeiter in ihrem jeweiligen Verantwortungsbereich bei der Einstellung und danach je nach Bedarf an den nötigen Sicherheitsschulungen teilnehmen

9.1.3 Mitarbeiter

Die Mitarbeiter haben die Aufgabe, ihren Teil zum Schutz von SAP und der Informationen und Assets ihrer Kunden und Partner beizutragen, indem sie unbefugten Zugriff und unsachgemäße Nutzung verhindern. Die Mitarbeiter sind außerdem für Folgendes verantwortlich:

- Den Zweck der Informationssicherheit verstehen und alle anwendbaren Security Policies und Standards einhalten
- SAP-Informationen gemäß dem *SAP Global Information Classification and Handling Standard* richtig klassifizieren und behandeln, um die Sicherheit der von ihnen verarbeiteten Internen und Vertraulichen Informationen zu gewährleisten

- Sicherheitsvorfälle oder andere Probleme in Bezug auf den Schutz oder den Missbrauch von Systemen gemäß dem Incident-Reporting-Prozess unverzüglich melden
- Alle anwendbaren Gesetze und Bestimmungen in ihrem jeweiligen Zuständigkeitsbereich einhalten
- An den vorgeschriebenen Sicherheitsschulungen teilnehmen
- Sicherstellen, dass sie sich nicht an Aktivitäten beteiligen, durch die Informationen oder IT-Infrastrukturen, die SAP oder ihren Kunden und Partnern gehören, unsachgemäß modifiziert, verändert, gelöscht oder genutzt werden können.

9.1.4 Externe Parteien

Externe Parteien, die Zugriff auf SAP-Informationen und -Assets erhalten, müssen vor Erteilung des Zugriffs eine geeignete Vereinbarung zum Schutz der Vertraulichkeit von SAP-Informationen unterzeichnen. Zu diesen Vereinbarungen zählen u. a. eine Geheimhaltungsvereinbarung (Non-Disclosure Agreement, NDA), das SAP Confidentiality and Privacy Statement (CPS), eine Servicevereinbarung oder eine Entwicklungsvereinbarung.

9.1.5 SAP Global Security

SAP Global Security ist für den Schutz der Marke, Mitarbeiter, Assets, Kundendaten und Informationstechnologie sowie des geistigen Eigentums von SAP vor Missbrauch oder Gefährdung verantwortlich.

9.1.6 SAP Security Steering Committee

Das SAP Security Steering Committee autorisiert die Inhalte dieser Policy. Dieses Gremium setzt sich aus leitenden Führungskräften und Vorstandsmitgliedern zusammen.

9.2 Funktionstrennung

Eine geeignete Funktionstrennung ist unabdingbar, um das Risiko von Betrug oder Missbrauch zu verringern. In Fällen in, denen eine Funktionstrennung nicht angewendet werden kann, müssen Kontrollen zur Eindämmung umgesetzt werden.

9.3 Kontakt zu Behörden

SAP Global Security muss Kontakte zu den zuständigen Behörden im Bereich Informationssicherheit pflegen und relevante Informationen an die betroffenen Geschäftseinheiten und Abteilungen weitergeben.

9.4 Kontakt zu speziellen Interessengruppen

Im Rahmen der jeweiligen Tätigkeit sind von SAP Global Security Kontakte zu entsprechenden Interessengruppen, Fachverbänden, Sicherheitsforen usw. zu pflegen.

9.5 Informationssicherheit im Projektmanagement

Der Informationssicherheit ist während aller Projektmanagementphasen Rechnung zu tragen, um sicherzustellen, dass Informationssicherheitsrisiken identifiziert und berücksichtigt werden. Während der Anfangsphasen von Projekten müssen Risikobeurteilungen durchgeführt werden.

10 RISIKOMANAGEMENT

Das Risikomanagement ist in die Managementprozesse zu integrieren und konsequent anzuwenden, um das richtige Maß an Sicherheit zu gewährleisten.

Ein Prozess zur Sicherheitsüberprüfung muss fester Bestandteil jeder System- oder Anwendungsentwicklung sein, um sicherzustellen, dass Sicherheitskontrollen in allen neuen Lösungen implementiert sind.

In regelmäßigen Abständen muss eine Risikoprüfung erfolgen, um die möglichen Risiken für wichtige Systeme zu beurteilen, die Vertrauliche Informationen von SAP beinhalten.

Weitere Anforderungen hinsichtlich des Risikomanagements und der Verantwortlichkeiten für entsprechende Aktivitäten sind in der *SAP Global Risk Management Policy* definiert.

11 PERSONALSICHERHEIT

11.1 Arbeitsverhältnis

Die Verantwortlichkeiten für Informationssicherheit sind an alle Mitarbeiter in den Beschäftigungsverträgen zu kommunizieren.

11.2 Hintergrundüberprüfungen

Alle Mitarbeiter müssen vor einer Beschäftigung gemäß den *SAP Background Verification Process Guidelines* und den entsprechenden Gesetzen, Richtlinien und Geschäftsanforderungen angemessen überprüft werden.

11.3 Beendigung oder Wechsel der Beschäftigung

Wenn ein interner oder externer Mitarbeiter gekündigt wird, die Stelle wechselt oder das Unternehmen verlässt, muss der logische und physische Zugang zeitnah aufgehoben oder geändert werden.

11.4 Sensibilisierung für Informationssicherheit, Sicherheitsschulungen

Alle internen und externen Mitarbeiter, die SAP-Informationen handhaben oder verarbeiten, müssen bei der Einstellung und danach jährlich durch regelmäßige Maßnahmen und Schulungen über ihre Verantwortung in Bezug auf Informationssicherheit unterrichtet werden.

12 SICHERHEIT VON MOBILEN GERÄTEN

SAP muss die mit der Nutzung von mobilen Geräten einhergehenden Risiken eindämmen, indem sie angemessene Kontrollen zum Schutz der SAP-Informationen anwendet, die verarbeitet oder gespeichert werden.

Alle mobilen Geräte, die Eigentum von SAP oder einzelnen Personen sind, und SAP-Informationen verarbeiten oder speichern, müssen durch eine Mobile-Device-Management-Lösung (MDM-Lösung) geschützt werden.

Technische Kontrollen müssen angewendet werden, um den Zugriff auf SAP-Informationen oder -Daten durch nicht autorisierte und/oder nicht verwaltete Anwendungen und Softwareprogramme auf mobilen Geräten zu kontrollieren.

Weitere Anforderungen hinsichtlich mobiler Geräte sind in der *SAP Mobile Device Security Procedure* und der *Acceptable Use Policy* definiert, die in diesem Dokument enthalten sind.

13 ASSET MANAGEMENT

SAP hat für alle ihre Assets, die im Informationslebenszyklus relevant sind, Verantwortlichkeiten sowie Pflichten zu deren Schutz identifiziert und definiert. Dieser Lebenszyklus umfasst die Erstellung, Verarbeitung, Speicherung, Übertragung, Löschung und Vernichtung von Informationen.

13.1 Verantwortlichkeit für Assets

Bei der Erstellung oder dem Erwerb von SAP-Assets müssen Asset-Verantwortliche identifiziert und definiert werden. Asset-Verantwortliche sind während des gesamten Lebenszyklus für Assets verantwortlich, u. a. für deren Inventarisierung, Klassifizierung, Handhabung, Schutz, Löschung oder Entsorgung sowie für das Management der sie betreffenden Zugriffskontrollen.

13.2 Asset-Inventar

Alle Assets, die Eigentum von SAP sind, müssen identifiziert und in einem Inventar erfasst werden, das genau geführt, regelmäßig aktualisiert und in festgelegten Zeitabständen überprüft wird. Das Inventar muss Auskunft über die Klassifizierungsstufe jedes Assets geben.

13.3 Zulässige Nutzung von Assets

Die Anforderungen hinsichtlich der zulässigen Nutzung von Assets sind in der *Acceptable Use Policy* definiert, die in diesem Dokument enthalten ist.

13.4 Rückgabe von Assets

Das Management trägt dafür Sorge, dass Assets bei Beendigung eines Beschäftigungsverhältnisses oder -vertrags, oder wenn sie nicht mehr zu Geschäftszwecken benötigt werden, zurückgegeben werden.

13.5 Klassifizierung von Assets

13.5.1 Sicherheitsklassifizierung von IT-Systemen

Jedes IT-System muss gemäß der Kritikalität der darin gespeicherten oder verarbeiteten Informationen als sicherheitskritisch oder nicht sicherheitskritisch klassifiziert werden.

Weitere Anforderungen hinsichtlich der Klassifizierung von IT-Systemen sind im *SAP IT Secure System Operation Standard* definiert.

13.5.2 Klassifizierung und Handhabung von Informationen

SAP-Informationen müssen als Vertraulich, Intern oder Öffentlich klassifiziert werden.

Informationsverantwortliche müssen SAP-Informationen auf der Grundlage ihrer Vertraulichkeit, ihrer Kritikalität, ihres Werts und der für sie geltenden gesetzlichen Anforderungen klassifizieren. Der Informationsverantwortliche stellt sicher, dass das Informations-Asset basierend auf seiner Klassifizierung entsprechend gekennzeichnet und geschützt ist, um unbefugten Zugriff darauf, Offenlegung, Änderung, Entfernung, Vernichtung oder unsachgemäße Nutzung zu verhindern.

Der Zugriff auf SAP-Informationen muss auf der Grundlage der geschäftlichen Anforderungen und nach dem Konzept der geringstmöglichen Rechte (Least Privilege Principle) erfolgen. Informationsbenutzer, die Zugriff auf SAP-Informationen erhalten haben, sind verpflichtet, die Informationen entsprechend der ihnen zugewiesenen Klassifikationsstufe zu handhaben.

Kategorie	Definition
Vertraulich	Hochsensible SAP-Informationen, die nur einer beschränkten Anzahl bestimmter Einzelpersonen zugänglich sind, bei denen ein definierter Zugriffsbedarf („Need to know“) vorliegt. Dazu zählen Informationen, die von SAP aufgrund von Gesetzen, Vorschriften und/oder Verträgen geschützt werden müssen sowie Informationen, die gemäß der *SAP Global Data Protection and Privacy Policy* als personenbezogene Daten gelten.
Intern	Sensible SAP-Informationen, die SAP-Mitarbeitern und autorisierten externen Mitarbeitern zugänglich sind, wobei jeglicher anderweitige Zugriff jedoch eingeschränkt und kontrolliert werden muss
Öffentlich	SAP-Informationen, die keines besonderen Schutzes bedürfen und öffentlich verbreitet werden können

Die Anforderungen hinsichtlich Klassifizierung, Kennzeichnung und Handhabung sind im *SAP Global Information Classification and Handling Standard* definiert.

13.6 Laptops und Arbeitsstationen

Alle SAP-Laptops und -Arbeitsstationen müssen durch eine zentrale Geräteverwaltungslösung verwaltet und geschützt werden und Folgendes aufweisen:

- ein SAP-Unternehmensbild
- verschlüsselte Datenspeicherung
- eine von SAP IT genehmigte Lösung zur Verschlüsselung von Daten auf Wechseldatenträgern

Die Anforderungen hinsichtlich der zulässigen Nutzung von Laptops und Arbeitsstationen sind in der *Acceptable Use Policy* definiert, die in diesem Dokument enthalten ist.

13.7 Datenspeichergeräte

SAP-Informationen, die auf Datenspeichergeräten gespeichert werden, müssen vor unbefugter Offenlegung, Qualitätsverschlechterung, Änderung, Entfernung und Vernichtung geschützt werden.

13.7.1 Wechseldatenträger

Die Anforderungen hinsichtlich der Nutzung von Wechseldatenträgern sind in der *Acceptable Use Policy* definiert, die in diesem Dokument enthalten ist.

13.7.2 Löschung und Entsorgung

Datenspeichergeräte, auf denen sich SAP-Informationen befinden, müssen gemäß sicheren und validierten Prozessen, die der Art des Geräts und der Vertraulichkeit der Informationen entsprechen, gelöscht und entsorgt werden.

Die enthaltenen Daten müssen während des gesamten Prozesses angemessen geschützt sein. Die Daten müssen sogar geschützt werden, nachdem das Gerät außer Betrieb genommen worden ist, oder wenn es der Nutzung für einen anderen geschäftlichen Zweck zugeführt wird. Datenaufbewahrungsanforderungen sind zu berücksichtigen.

13.8 Transport von physischen Medien

Physische Medien, die SAP-Informationen enthalten, beispielsweise Papierdokumente, DVDs oder Wechseldatenträger, müssen während des Transports sicher sein.

Datenspeichergeräte, die Vertrauliche SAP-Informationen enthalten, müssen mit einem international anerkannten Verfahren, das als sicher gilt, verschlüsselt werden. Ihr Transport

muss dokumentiert werden und rückverfolgbar sein. Die Informationen für die Entschlüsselung müssen über einen anderen Kommunikationskanal übertragen werden.

14 ZUGRIFFSVERWALTUNG

Der auf SAP-IT-Systeme und das SAP-Netzwerk erteilte Zugriff erfordert die Anwendung von Zugriffskontrollen, die den gesetzlichen und vertraglichen Pflichten, dem Sicherheitsrisiko und den geschäftlichen Anforderungen Rechnung tragen.

Formale Prozesse sind zu etablieren, um:

- Nicht autorisierten Zugriff zu verhindern
- Die Anmeldung und Abmeldung von Berechtigungen zu regeln
- Berechtigungen bereitzustellen
- Besondere Zugriffsrechte einzuschränken und zu kontrollieren
- Intervalle für die Überprüfung von Zugriffsrechten zu etablieren
- Bei Beendigung des Beschäftigungsverhältnisses, des Vertrags oder der Vereinbarung Benutzern Zugriffsrechte verlässlich zu entziehen
- Den Einsatz von Hilfsprogrammen, die die System- und Anwendungssteuerung aufheben können, einzuschränken und zu kontrollieren
- Den Zugang zum Quellcode von Programmen zu beschränken
- Den Zugriff auf Systeme und Anwendungen ggf. über ein sicheres Anmeldeverfahren zu kontrollieren
- Allen SAP-Systembenutzern die Verantwortung für den Schutz von Authentifizierungsinformationen zu übertragen
- Sicherzustellen, dass alle Kennwörter den festgelegten Komplexitätsvoraussetzungen entsprechen
- Den Zugriff und die sichere Registrierung externer Parteien zu verwalten und sicherzustellen

15 FERNZUGRIFF

SAP IT muss die Anforderungen definieren, die erfüllt sein müssen, um die Risiken in Verbindung mit dem Arbeiten außerhalb von SAP-Standorten zu steuern. Der Zugriff auf das SAP Corporate Network von Remote-Hosts oder -Netzwerken muss mithilfe von definierten Zwei-Faktor-Authentifizierungskriterien und verschlüsselten Verbindungen beschränkt und kontrolliert werden.

16 KRYPTOGRAFISCHE VERFAHREN

16.1 Kryptografische Kontrollmechanismen

SAP verwendet Verschlüsselung, um die Vertraulichkeit und Integrität von SAP-Informationen zu schützen.

Die Nutzung von Verschlüsselung zum Schutz von Vertraulichen SAP-Informationen muss den Branchenstandards, vertraglichen Verpflichtungen gegenüber Kunden sowie staatlichen Import- und Exportrichtlinien entsprechen. Alle Verschlüsselungsverfahren müssen international anerkannt sein und als sicher gelten.

16.2 Schlüsselverwaltung

Kryptografieschlüssel müssen während ihres gesamten Lebenszyklus verwaltet und geschützt werden; dieser umfasst ihre Erstellung, Speicherung, Archivierung, ihren Abruf, ihre Verteilung, Stilllegung und Vernichtung.

Weitere Anforderungen hinsichtlich kryptografischer Verfahren sind im *SAP IT Secure System Operation Standard* definiert.

17 PHYSISCHE UND UMGEBUNGSBEZOGENE SICHERHEIT

Physische Sicherheitsmaßnahmen müssen implementiert werden, um die Menschen zu schützen, die Integrität von Betriebsstätten und Informationsverarbeitungszentren aufrechtzuerhalten sowie den nicht autorisierten Abfluss von SAP-Informationen und den Verlust von Assets zu kontrollieren.

Der Schutz von Menschenleben hat Vorrang vor allen anderen Sicherheitsmaßnahmen.

Die bereitgestellten Schutzmaßnahmen müssen zu den identifizierten Risiken sowie der Klassifizierungsstufe und dem Wert der Assets und SAP-Informationen im Verhältnis stehen.

Weitere Anforderungen hinsichtlich der physischen Sicherheit sind im *SAP Global Physical Security Standard* und in der *Acceptable Use Policy* definiert, die in diesem Dokument enthalten sind.

18 BETRIEBSSICHERHEIT

SAP muss den sicheren Betrieb von Systemen gewährleisten, um die Vertraulichkeit, Integrität und Verfügbarkeit der von ihr verarbeiteten Informationen zu schützen.

Für die folgenden Punkte sind formale Prozesse zu etablieren:

- Dokumentation und Pflege von Betriebsabläufen
- Änderungsmanagement
- Kapazitätsmanagement
- Trennung von produktiven und nicht produktiven Umgebungen
- Schutz vor Schadsoftware
- Sicherung und Wiederherstellung
- Protokollierung und Überwachung
- Uhrensynchronisation
- Kontrolle der Betriebssoftware
- Schwachstellen-Management
- Überlegungen zu Systemprüfungen
- Installation von Software

19 KOMMUNIKATIONSSICHERHEIT

19.1 Management der Netzwerksicherheit

Kontrollen müssen angewendet werden, um die Sicherheit des SAP-Netzwerk und der mit ihm verbundenen IT-Systeme sicherzustellen sowie Informationen während der Übermittlung gegen Abfangen, Veränderung und Löschung zu schützen.

Weitere Anforderungen hinsichtlich Netzwerksicherheit sind im *SAP IT Secure System Operation Standard* definiert.

19.2 Informationsübertragung

SAP muss die Übertragung von Informationen schützen, um sicherzustellen, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Kommunikation während der gesamten Übertragung aufrechterhalten bleibt. Alle IT-Systeme sind so zu konfigurieren, dass sie gemäß dem Schutzbedarf der übertragenen Informationen eine sichere Kommunikation nutzen.

Weitere Anforderungen hinsichtlich der Informationsübertragung sind im *SAP IT Secure System Operation Standard* und im *SAP Global Information Classification and Handling Standard* definiert.

19.2.1 Elektronische Kommunikation

SAP muss geeignete Kontrollen implementieren, um die SAP-Informationen und -Daten zu schützen, die über elektronische Kommunikationswege wie etwa E-Mail- und Messaging-Anwendungen und -Software übertragen werden.

Sämtliche Fremdanwendungen und -softwareprogramme, die verwendet werden, um SAP-Informationen, -Daten oder geschäftsrelevante Mitteilungen zu übertragen oder zu kommunizieren, müssen von SAP IT autorisiert werden. SAP muss sicherstellen, dass Datenaufbewahrungs- und Datenschutzanforderungen sowie andere geltende gesetzliche und behördliche Vorschriften als Teil des Autorisierungsprozesses betrachtet werden.

Alle autorisierten Anwendungen und Softwareprogramme, die verwendet werden, um SAP-Informationen, -Daten oder geschäftsrelevante Mitteilungen über ein mobiles Gerät zu übertragen oder zu kommunizieren, müssen durch eine Mobile-Device-Management-Lösung (MDM-Lösung) von SAP verwaltet werden.

Weitere Anforderungen hinsichtlich der elektronischen Kommunikation bei SAP sind in der *Acceptable Use Policy* dargelegt, die in diesem Dokument enthalten ist.

19.2.2 Vereinbarungen zur Informationsübertragung

Die Übertragung von Informationen zwischen SAP und externen Parteien muss in entsprechenden Vereinbarungen, einschließlich sämtlichen erforderlichen Datenschutzvereinbarungen, geregelt werden.

Vertrauliche und Interne SAP-Informationen dürfen externen Parteien gegenüber nicht offengelegt werden, es sei denn, es gilt eine Geheimhaltungsvereinbarung (NDA) oder eine andere geeignete Vertraulichkeitsvereinbarung.

20 SICHERE ENTWICKLUNG UND SICHERER ERWERB

Sicherheit muss in SAP-IT-Systemen und -Anwendungen über den gesamten Entwicklungslebenszyklus hinweg integriert sein. Es müssen Anforderungen hinsichtlich der Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit der enthaltenen Informationen während aller Phasen der Entwicklung definiert und umgesetzt werden; diese umfassen Anwendungs- und Systemrisikobeurteilung, Planung, Entwicklung oder Erwerb, Modifizierung, Tests, Validierung und Korrekturmaßnahmen.

Weitere Anforderungen hinsichtlich von SAP entwickelter Anwendungen sind im *SAP Product Security Standard* definiert.

21 SICHERHEIT IN LIEFERANTENBEZIEHUNGEN

Alle relevanten Lieferanten, Partner und Dienstleister sind verpflichtet, bei der Erbringung von Dienstleistungen die in den vertraglichen Vereinbarungen festgelegten Sicherheitsmaßnahmen umzusetzen.

SAP muss die mit dem Zugriff von Lieferanten auf Informationen und Assets des Unternehmens verbundenen Risiken durch folgende Maßnahmen eindämmen:

- Definieren der Sicherheitsanforderungen in Lieferantenvereinbarungen
- Ermitteln der Risiken, die im Zusammenhang mit der Lieferkette in der Informations- und Kommunikationstechnologie bestehen
- Überwachen der Servicebereitstellung durch Lieferanten
- Kontrollieren von Änderungen an Services von Lieferanten

Weitere Anforderungen hinsichtlich externer Parteien und Lieferanten sind im *SAP Supplier Security Standard* und im *SAP IT Secure System Operation Standard* definiert.

22 MAßNAHMEN BEI UND MANAGEMENT VON SICHERHEITSVORFÄLLEN

Für die Meldung und das Management von Sicherheitsvorfällen müssen Anforderungen definiert und umgesetzt werden, die eine zeitnahe und effektive Reaktion auf Sicherheitsvorfälle sicherstellen.

Diese Anforderungen müssen dokumentiert, gepflegt, geprüft und regelmäßig getestet werden. Diese Anforderungen müssen Folgendes beinhalten:

- Zuständigkeiten beim Vorfallmanagement
- Vorgehensweisen beim Sammeln und Aufbewahren von Beweismitteln
- Prozesse für das Melden von Sicherheitsvorfällen
- Prozessabläufe für die Vorbereitung, Aufdeckung, Analyse, Eindämmung, Meldung, Preisgabe und Wiederherstellung
- Aktivitäten nach einem Sicherheitsvorfall zur Erfassung von Erfahrungswerten

Die Anforderungen hinsichtlich der Meldung von Sicherheitsvorfällen durch Mitarbeiter sind in der *Acceptable Use Policy* definiert, die in diesem Dokument enthalten ist.

23 GESCHÄFTSKONTINUITÄT

SAP muss ein Notfallmanagement-Programm aufrechterhalten, um bei Eintreten eines Störfalls die Fortführung bzw. Wiederherstellung des Geschäftsbetriebs in angemessener Weise sicherzustellen. Das Programm für Geschäftskontinuität bei SAP umfasst Disaster Recovery, IT-Service-Kontinuität, Prozesskontinuität und Krisenmanagement. Dieses Programm muss Folgendes abdecken:

- Identifizieren kritischer Assets
- Festlegen der Zeitrahmen für die Wiederherstellung
- Definieren der Anforderungen für den Schutz von Assets
- Aufrechterhalten der Kontinuität der Informationssicherheit

Für jede Geschäftseinheit, jeden IT-Service und jeden kritischen Prozess muss ein Plan gepflegt werden, der die Sicherheitsanforderungen für den Schutz von SAP-Informationen und -Assets während Unterbrechungen des Geschäftsbetriebs regelt. Diese Pläne müssen zur Vorbereitung auf unvorhersehbare Bedrohungen des Geschäftsbetriebs dokumentiert, gepflegt, geprüft und regelmäßig getestet werden.

Weitere Anforderungen hinsichtlich der Geschäftskontinuität sind im *SAP Business Continuity and Operational Resilience Standard* und im *SAP Global Physical Security Standard* definiert.

24 EINHALTUNG VON SICHERHEITSANFORDERUNGEN

SAP muss durch regelmäßige Überprüfung ihrer Sicherheits- und Kontrollumgebung dafür sorgen, dass betriebliche, gesetzliche bzw. behördliche und vertragliche Sicherheitsanforderungen eingehalten werden.

24.1 Gesetzliche und vertragliche Anforderungen

Vertragliche Verpflichtungen sowie lokale und internationale gesetzliche Vorschriften müssen in Zusammenarbeit mit den verantwortlichen SAP-Organisationseinheiten identifiziert, dokumentiert und eingehalten werden.

24.1.1 Schutz von Datensätzen

Datensätze müssen gemäß gesetzlichen, behördlichen, vertraglichen und geschäftlichen Vorschriften vor Verlust, Vernichtung, Qualitätsverschlechterung, Fälschung, unbefugtem Zugriff und nicht autorisierter Freigabe geschützt werden.

SAP muss Anforderungen für die Aufbewahrung, Speicherung, Inventarisierung, Handhabung und Entsorgung von Datensätzen und SAP-Informationen definieren.

Weitere Anforderungen hinsichtlich des Schutzes von Datensätzen sind in der *SAP Information Governance and Records Management Policy* definiert.

24.1.2 Datenschutz

SAP muss den Schutz und die ordnungsgemäße Handhabung der personenbezogenen Daten sicherstellen, die sie erfasst, verarbeitet oder nutzt.

Das SAP Data Protection and Privacy Office (DPPO) trägt dafür Sorge, dass SAP die geltenden Bestimmungen des Datenschutzgesetzes einhält. Lokale Gesetze machen gegebenenfalls zusätzliche Anforderungen in Bezug auf die Handhabung notwendig.

Jeder Mitarbeiter ist für die sichere Handhabung von personenbezogenen Daten verantwortlich; hierzu können auch Kunden- und/oder Partnerinformationen gehören.

Weitere Anforderungen hinsichtlich des Datenschutzes sind im *SAP Global Information Classification and Handling Standard* und in der *SAP Global Data Protection and Privacy Policy* definiert.

24.1.3 Geistiges Eigentum

Verfahren zum Schutz von Rechten an geistigem Eigentum müssen gemäß vertraglichen Verpflichtungen sowie lokalen und internationalen Gesetzen und Vorschriften angewendet werden.

24.2 Überprüfungen der Informationssicherheit

24.2.1 Unabhängige Überprüfung

Sicherheitsbezogene Zertifizierungen und/oder Nachweise, die von unabhängigen Auditorganisationen ausgestellt wurden, müssen aufbewahrt werden.

24.2.2 Einhaltung der SAP Security Policies und SAP Security Standards

Interne Überprüfungen von Sicherheitskontrollen müssen durchgeführt werden, um die Einhaltung von SAP-Policies und -Standards sicherzustellen. Alle festgestellten Verstöße müssen auf Korrekturmaßnahmen hin evaluiert werden.

24.2.3 Technische Überprüfung

SAP-IT-Systeme und -Netzwerke müssen regelmäßig auf Konformität mit technischen Sicherheitsanforderungen überprüft werden.

Prozesse für die Durchführung sicherer Code-Überprüfungen auf von SAP entwickelten Anwendungen müssen definiert und eingehalten werden.

Penetrationstests für Anwendungen und/oder die Infrastruktur müssen auf der Grundlage der Anfälligkeit und der Kritikalitätseinstufung der Anwendung oder der Infrastruktur erfolgen.

Regelmäßige Schwachstellprüfungen sind laut den geschäftlichen Anforderungen durchzuführen. Die Maßnahmen zur Schwachstellenbehebung orientieren sich an der Risikostufe und der Kritikalität der Schwachstelle. Anwendungen und Systeme müssen je nach Kritikalität der Schwachstelle nachgebessert werden. Entscheidende Schwachstellen müssen so schnell wie möglich behoben werden.

Weitere Anforderungen hinsichtlich von SAP entwickelter Anwendungen sind im *SAP Product Security Standard definiert.*

25 ACCEPTABLE USE POLICY (GRUNDSÄTZE FÜR DIE ZULÄSSIGE NUTZUNG)

SAP bestimmt die angemessenen Verhaltensweisen und Maßnahmen bei der Nutzung von SAP-Informationen und Assets. Alle Mitarbeiter und externen Parteien, die SAP-Informationen oder -Assets verarbeiten, darauf zugreifen oder anderweitig nutzen, müssen die folgenden Anforderungen einhalten.

25.1 Verbotene Aktivitäten

Die folgenden Handlungen sind verboten:

- Jede unbefugte Nutzung von SAP-IT-Systemen, SAP-Informationen, Kunden- und/oder Partnerinformationen.
- Die absichtliche Teilnahme an Aktivitäten, die die Informationssicherheit, die IT-Systeme oder Netzwerke von SAP oder seiner Kunden, Partner oder externer Parteien gefährden könnten.
- Die Beteiligung an jeglichen Aktivitäten, die laut lokalem, regionalem, staatlichem oder internationalem Recht unzulässig sind und für die SAP-Ressourcen genutzt werden.
- Die Verletzung der Rechte des geistigen Eigentums einer Person oder eines Unternehmens.
- Nicht autorisierte Versuche, die Sicherheitskonfiguration eines SAP-IT-Systems zu verändern oder die Sicherheitseinschränkungen zu umgehen oder zu deaktivieren, um sich Zugriff auf geschützte Informationen oder Bereiche zu verschaffen.
- Die Verwendung von SAP-IT-Systemen, um anstößige Inhalte herunterzuladen, zu speichern oder zu übermitteln. Anstößige Inhalte sind u. a. pornographische, beleidigende, diskriminierende, rassistische oder diffamierende Materialien
- Die Verwendung von SAP-IT-Systemen, um illegale, urheberrechtlich geschützte oder nicht lizensierte Software, Informationen, Musik oder andere Multimediadateien zu erstellen, herunterzuladen, zu speichern, zu verkaufen, zu verteilen, zu kopieren oder auszutauschen.
- Das vorsätzliche Löschen oder Vernichten von SAP-Informationen, -Kommunikation oder -Datensätzen, die unter den Schutz durch die *SAP Information Governance and Records Management Policy*, die *SAP Global Data Protection and Privacy Policy* oder andere gesetzliche und behördliche Vorschriften fallen.
- Die Nutzung von Anwendungen oder Software (einschließlich Ephemeral-Messaging-Anwendungen), die von SAP IT nicht für die Kommunikation über geschäftsrelevante Belange von SAP autorisiert wurden.
- Die Verwendung jeder Art von Tools, Anwendungen und Geräten oder Exploits (Ausnutzung von Schwachstellen), um in unzulässiger Weise auf SAP-Informationen zuzugreifen.

25.2 Private Nutzung von SAP-Geräten

SAP-Endbenutzergeräte und -Sprachkommunikationseinrichtungen dürfen zur gelegentlichen privaten Nutzung verwendet werden. Die private Nutzung dieser Geräte unterliegt den gleichen Vorschriften wie die geschäftliche Nutzung.

Jegliche Nutzung muss gemäß dem *SAP Code of Business Conduct for Employees* und den Anforderungen für die Handhabung von SAP-Informationen, wie sie im *SAP Global Information Classification and Handling Standard* aufgeführt sind, erfolgen.

Die private Nutzung von zentralen IT-Systemen oder -Servern, die primär für die Verarbeitung, die Massenspeicherung und den Austausch von SAP-Informationen und -Daten eingesetzt werden, ist nicht erlaubt. Private Dateien dürfen nicht auf diesen Systemen gespeichert werden.

Jegliche private Nutzung von SAP-Geräten darf sich nicht negativ auf die Produktivität, Systemverfügbarkeit oder Performance auswirken.

25.3 Laptops und Arbeitsstationen

25.3.1 Sperren von Laptops und Arbeitsstationen

Laptops und Arbeitsstationen von SAP sind zu sperren, wenn sie unbeaufsichtigt gelassen werden, und zwar auch dann, wenn es nur für kurze Zeit ist. (Mit ⊞ + L lässt sich beispielsweise auf Windows-Computern der Bildschirm sperren.) Die zeitabhängige Sperre von Geräten darf nicht deaktiviert werden.

25.3.2 Unbefugter Zugriff

Unbefugten Benutzern darf der Zugriff auf SAP-Laptops oder -Arbeitsstationen nicht gewährt werden.

25.3.3 Sicherheits-Updates und Patches

Das Weitergeben von Sicherheitsupdates (Patches) ist ein automatischer Prozess. Sicherheits- und Betriebssystem-Updates müssen auf allen SAP-Laptops oder -Arbeitsstationen akzeptiert werden. Außerdem muss das Update durch den Neustart des Geräts unterstützt werden.

25.3.4 Backups

Für SAP-Laptops und -Arbeitsstationen muss der von SAP IT bereitgestellte Backup-Service verwendet werden. SAP-Informationen dürfen nicht auf privaten Geräten gesichert werden.

25.3.5 Installation von Software und Anwendungen

Sämtliche Softwareprogramme und Anwendungen auf SAP-Laptops und -Arbeitsstationen müssen von einem Software-Store von SAP IT bezogen werden oder anderweitig von SAP autorisiert sein.

Nicht autorisierte oder illegale Kopien von Software auf SAP-Laptops und -Arbeitsstationen müssen auf eine E-Mail-Benachrichtigung von SAP IT hin unverzüglich gelöscht werden.

25.3.6 Private Arbeitsstationen und Laptops

Private Arbeitsstationen und Laptops dürfen nicht verwendet werden, um SAP-Informationen zu verarbeiten und/oder darauf zuzugreifen, sofern der externe Zugriff nicht über einen von SAP IT genehmigten Virtual Desktop erfolgt. Private Arbeitsstationen und Laptops dürfen nicht verwendet werden, um SAP-Informationen aus SAP-Systemen zu exportieren und/oder SAP-Informationen zu speichern.

Die Nutzung von privaten mobilen Geräten, z. B. Smartphones oder Tablets, für geschäftliche Zwecke bei SAP ist an anderer Stelle in dieser Policy geregelt.

25.4 Wechseldatenträger

Wechseldatenträger dürfen bei SAP geschäftlich zur vorübergehenden Übertragung oder Sicherung von Informationen genutzt werden, aber nur, wenn keine andere Möglichkeit zur Verfügung steht.

Vertrauliche SAP-Informationen, die auf Wechseldatenträgern gespeichert sind, müssen mit einer von SAP IT genehmigten Methode verschlüsselt werden. Der Transport muss dokumentiert werden, und der Verbleib der Geräte muss jederzeit bekannt sein. Die für die Entschlüsselung benötigten Informationen müssen dem Empfänger auf einem anderen Kommunikationsweg übermittelt werden als der Wechseldatenträger.

Jeder Wechseldatenträger, der mit SAP-Endbenutzergeräten verwendet wird, oder jedes private mobile Gerät, das geschäftlich bei SAP verwendet wird, muss aus einer bekannten und zuverlässigen Quelle stammen.

25.5 Mobile Geräte

Weitere Anforderungen an die Sicherheit mobiler Geräte sind in der *Mobile Device Handling Procedure* beschrieben.

25.5.1 Nutzung von privaten mobilen Geräten

Die Nutzung privater Mobilgeräte für die geschäftliche Nutzung bei SAP ist zulässig, wenn ihre Nutzung im Land des Mitarbeiters erlaubt und durch die Mobile-Device-Management-Lösung (MDM) von SAP IT gesichert ist.

Private Mobilgeräte, die geschäftlich bei SAP genutzt werden, dürfen nicht gefährdet sein (etwa durch Jailbreaking oder Rooting).

Vor der Entsorgung oder dem Verkauf eines privaten Mobilgeräts, das geschäftlich bei SAP genutzt worden ist, müssen entweder alle SAP-Informationen von dem Gerät gelöscht werden oder das Gerät muss anderweitig dauerhaft unbrauchbar gemacht werden.

25.5.2 Sicherheits-Updates und Patches

Sicherheits- und Betriebssystem-Patches und -Updates müssen installiert werden, sobald sie zur Verfügung gestellt worden sind. Ebenso müssen Anwendungen aktualisiert werden, sobald Updates zur Verfügung stehen.

25.5.3 Installation von Software und Anwendungen

Anwendungen auf mobilen Geräten von SAP oder auf privaten Mobilgeräten, die geschäftlich bei SAP genutzt werden, müssen von offiziellen App-Store-Anbietern (z. B. Apple oder Google Play) oder von einem von SAP IT verwalteten Mobile-App-Store bezogen werden.

Sämtliche Fremdsoftware und Anwendungen Dritter, die verwendet werden, um SAP-Daten, -Informationen oder geschäftsrelevante Mitteilungen zu übertragen oder zu kommunizieren, müssen von SAP IT autorisiert werden.

Nicht autorisierte oder illegale Kopien von Software auf mobilen Geräten von SAP müssen auf eine E-Mail-Benachrichtigung von SAP IT hin unverzüglich gelöscht werden.

25.6 Beschaffung von Hardware

SAP-Hardware muss gemäß dem Standardprozess von SAP IT und des Global Procurement Office bestellt und bezogen werden.

25.7 Diebstahlschutz

Laptops, Wechseldatenträger und mobile Geräte, die geschäftlich bei SAP genutzt werden, dürfen an Orten, an denen sie leicht entwendet werden können, nicht unbeaufsichtigt gelassen werden.

Der Verlust oder Diebstahl eines der vorgenannten Geräte muss unverzüglich über das SAP-GSIM-Tool (Global Security Incident Management) im SAP Corporate Portal gemeldet werden.

25.8 Schutz vor Malware

25.8.1 Virenschutzsoftware

Virenschutzsoftware darf nicht deaktiviert, verändert oder neu konfiguriert werden.

Regelmäßige, umfassende Virenprüfungen oder die automatische Aktualisierung der Virenschutzsoftware sollten möglichst ungehindert ablaufen können. Wenn die Prüfung oder Aktualisierung aus irgendeinem Grund aufgeschoben werden muss, ist sie innerhalb von 48 Stunden wieder aufzunehmen.

Die Benutzer sind verpflichtet, SAP IT Services zu benachrichtigen, wenn die Virenschutz-software nicht funktioniert oder anderweitig die Produktivität beeinträchtigt.

25.8.2 Virenprüfung von externen Informationen

Die von SAP IT Services bereitgestellte Virenschutzsoftware muss eingesetzt werden, um Software, Informationen und Datenträger aus externen Quellen vor deren Nutzung auf Viren zu überprüfen.

25.8.3 Verdacht auf Schadsoftware

Wenn der Verdacht besteht, dass ein SAP-Endbenutzergerät oder anderes SAP-IT-System mit Malware infiziert worden ist, muss der Benutzer dies unverzüglich über das SAP-GSIM-Tool (Global Security Incident Management) im SAP Corporate Portal melden.

25.9 Überwachung

Internetzugriff und Kommunikation können zu Diagnose-, Sicherheits- und Abrechnungszwecken von der IT protokolliert werden.

25.10 Anforderungen bei Reisen

25.10.1 Besitz von Geräten und Informationen

SAP-Informationen und -Geräte – u. a. Papierdokumente, Laptops, Mobilgeräte und Wechseldatenträger –, die verwendet werden, um SAP-Geschäfte zu tätigen, sind auf Reisen jederzeit bei sich zu führen. Die Informationen und Geräte dürfen nicht als Gepäck aufgegeben werden. Die einzige Ausnahme von dieser Regel stellen etwaige Bestimmungen von Fluggesellschaften oder Behörden dar, wonach Laptops als Reisegepäck aufgegeben werden müssen.

Der Verlust, die Pfändung oder der Diebstahl der vorgenannten Informationen bzw. Geräte ist unverzüglich über das SAP-GSIM-Tool (Global Security Incident Management) im SAP Corporate Portal zu melden.

Wenn Zoll- oder Strafverfolgungsbeamte die Entschlüsselung eines SAP-Laptops oder eines für SAP geschäftlich genutzten Wechseldatenträgers oder Mobilgeräts verlangen, muss dieser Vorfall unverzüglich als potenzielle Gefährdung von SAP-Informationen über das SAP-GSIM-Tool (Global Security Incident Management) im SAP Corporate Portal gemeldet werden.

25.10.2 Kennwörter und Web-Browser

Benutzer werden dazu angehalten, den Web-Browserverlauf, einschließlich Chronik, Cache, Cookies, URLs und temporärer Dateien, nach jeder Reise zu löschen.

Bei ihrer Rückkehr von Auslandsreisen werden die Benutzer gebeten, alle Kennwörter und PINs auf dem SAP-Laptop oder dem für SAP geschäftlich genutzten mobilen Gerät zu ändern.

25.11 Internetnutzung

Filter werden gesetzt, um den Zugriff auf bestimmte Seiten zu verhindern. Wenn jedoch Benutzer feststellen, dass sie auf eine Website zugegriffen haben, die pornographische, rassistische oder womöglich anstößige Inhalte enthält, müssen sie sofort die Verbindung abbrechen.

Die Nutzung von Internet-Services zum Übertragen, Weiterleiten oder anderweitigen Erstellen, Teilen oder Verbreiten von Informationen, die zum Nachteil der Interessen oder des Ansehens von SAP sein könnten, ist verboten.

Jedwede Nutzung von Internet-Services, die Gesetzen oder Vorschriften widersprechen, ist verboten.

25.12 Soziale Medien

Jegliche Nutzung von sozialen Medien unterliegt den *SAP Social Media Guidelines*.

25.13 Kommunikation

Weitere Anforderungen hinsichtlich der Kommunikation von SAP-Informationen sind im *SAP Global Information Classification and Handling Standard* dargelegt.

25.13.1 Sprachkommunikationssysteme

Konferenzbrücken dürfen nur dann im aktivierten Zustand sein, wenn sie verwendet werden.

Alle Parteien müssen vorab darüber informiert werden, falls Gespräche aufgezeichnet werden.

25.13.2 Voicemail

Die Mailbox-PIN muss geändert werden:

- Wenn eine Mailbox zum ersten Mal genutzt wird
- Wenn es Anlass zur Befürchtung gibt, dass die PIN nicht mehr sicher ist
- In regelmäßigen Abständen

Es ist verboten, Vertrauliche und Interne SAP-Informationen auf Anrufbeantwortern oder Voicemail-Systemen zu hinterlassen, deren Sicherheit nicht gewährleistet ist.

25.13.3 Faxnachrichten

Faxübertragungen von SAP-Dokumenten müssen gemäß den im *SAP Global Information Classification and Handling Standard* dargelegten Anforderungen erfolgen.

25.13.4 Elektronische Kommunikation

Jede Person ist für die Aktivitäten und die Nutzung des ihr zugewiesenen E-Mail- oder Messaging-Kontos rechenschaftspflichtig.

Elektronische SAP-Daten, -Informationen und geschäftsrelevante Mitteilungen dürfen nur über folgende Wege übertragen oder kommuniziert werden:

- Von SAP bereitgestellte E-Mail- und Messaging-Systeme
- Von SAP IT autorisierte Fremdanwendungen und -software
- Kundeninitiierte Messaging-Systeme, die den vertraglichen Verpflichtungen entsprechen

Weitere Anforderungen hinsichtlich elektronischer Kommunikation sind im *SAP Global Information Classification and Handling Standard* dargelegt.

Messaging-Anwendungen

Die Aufbewahrungs- und Löscheinstellungen in autorisierten Messaging- und Social-Media-Anwendungen von Fremdanbietern, die geschäftlich für SAP genutzt werden, müssen so konfiguriert sein, dass Nachrichten gemäß der *SAP Information Governance and Records Management Policy*, der *SAP Global Data Protection and Privacy Policy* und anderen gesetzlichen und behördlichen Vorschriften aufbewahrt werden.

Weitere Anforderungen hinsichtlich der Handhabung von Informationen in Messaging-Anwendungen sind im *SAP Global Information Classification and Handling Standard* dargelegt.

E-Mail

SAP-E-Mail-Nachrichten dürfen nicht automatisch auf externe Messaging-Systeme umgeleitet bzw. an diese weitergeleitet werden.

Bevor Anhänge oder Hyperlinks von unbekannten Absendern geöffnet werden, ist dieser Schritt sorgfältig zu bedenken.

Es ist verboten, E-Mail-Anhänge zu öffnen, zu versenden oder weiterzuleiten, die vermutlich Viren oder sonstige Inhalte enthalten, die SAP oder ihre Kunden oder Partner schädigen könnten.

Viruswarnungen dürfen nicht an Kollegen weitergeleitet werden. Bedenken bezüglich Viruswarnungen sollten über das GSIM-Tool (Global Security Incident Management) im SAP Corporate Portal gemeldet werden.

E-Mails müssen basierend auf ihren Inhalten und Anhängen gemäß dem *SAP Global Information Classification and Handling Standard* klassifiziert werden.

25.13.5 Inakzeptable Inhalte

Es ist verboten, SAP-E-Mail- oder -Messaging-Systeme zu verwenden, um Kommunikation zu senden oder zu beantworten, die Folgendes enthält:

- Inhalte, die als anstößig, bedrohlich, illegal oder belästigend betrachtet werden können, darunter sexuelle Anspielungen oder Bilder, rassistische Beschimpfungen oder andere Bemerkungen bzw. Bilder, die eine Person aufgrund seiner oder ihrer Rasse, der Herkunft, dem Geschlecht, der sexuellen Orientierung, der Religionszugehörigkeit, der politischen Überzeugung, einer Behinderung usw. beleidigen würden
- SPAM-Nachrichten, Kettenmails oder Pyramidensysteme jeder Art

25.14 Kennwörter

25.14.1 Anforderungen für Kennwörter

Alle Kennwörter oder PINs müssen die im *SAP IT Secure System Operation Standard* definierten Mindestanforderungen erfüllen.

25.14.2 Empfehlungen für sichere Kennwörter

Der Gebrauch von Wörtern, die auch im Wörterbuch zu finden sind, egal in welcher Sprache, auch von umgangssprachlichen, Dialekt- oder Jargon-Wörtern, ist zu vermeiden (auch rückwärts geschrieben oder bei Hinzufügen einer Zahl oder eines Sonderzeichens, wie beispielsweise in „secret1“).

Die Angabe von persönlichen Informationen ist zu vermeiden (z. B. Geburtsdatum, Familiennamen oder Haustiere).

Kennwörter, die auf den ersten Buchstaben eines Liedtitels, einer Affirmation oder eines anderen Satzes basieren und mit Zahlen und Sonderzeichen kombiniert werden, sind in Erwägung zu ziehen. Lautet der Satz beispielsweise „This May Be One Way To Remember“, dann könnte als Kennwort unter anderem „TmB1w2R!“ oder „Tmb1W>r~“ genutzt werden.

25.14.3 Kennwortschutz

SAP-Systemkennwörter, Benutzerzertifikate für Single Sign-On (SSO), PINs oder andere für SAP-IT-Systeme oder -Anwendungen genutzte Kennwörter dürfen nicht an Personen weitergegeben werden, die nicht ausdrücklich zu deren Verwendung autorisiert sind.

Kennwörter oder PINs dürfen nie auf Papier festgehalten oder in lesbarer Form aufbewahrt werden. Die Benutzer sind stattdessen angehalten, ein sicheres Kennwortmanagementsystem zu verwenden.

Muss ein Kennwort für ein kennwortgeschütztes Dokument oder ein Demosystem gemeinsam genutzt werden, so ist das Kennwort getrennt vom Dokument und den anderen Anmeldeinformationen zu versenden. Ein Kennwort darf nie zusammen mit dem Dokument oder dem Konto, das es entsperrt, ausgegeben werden.

Die Kennworteingabe darf nicht mithilfe automatischer Anmeldung, einer Anwendungserinnerung, integrierter Skripte oder fest programmierter Kennwörter in Client-Software übersprungen werden.

PINs und Kennwörter dürfen nicht auf öffentlichen Computern gespeichert werden. Zudem sind Browser-Cache und -Verlauf nach dem Trennen der Verbindung zu Computern, die auch für andere zugänglich sind, zu löschen. Auf diese Weise soll verhindert werden, dass nicht

autorisierte Personen Zugang zu Kennwörtern, PINs und weiteren Anmeldeinformationen erhalten.

Es sollte nicht das gleiche Kennwort für SAP- und private Konten genutzt werden.

Kennwörter und PINs müssen umgehend geändert werden, wenn irgendein Verdacht besteht, dass ein Kennwort oder eine PIN nicht mehr sicher sein könnte.

Wenn ein Dritter nach dem Kennwort oder der PIN fragt, muss dies über den Incident-Reporting-Prozess sofort als Sicherheitsvorfall und als mögliche Gefährdung von SAP-Informationen gemeldet werden.

25.15 Clean Desk und Clear Screen

Alle Mitarbeiter und externen Parteien müssen die Vorschriften bezüglich der Handhabung von SAP-Informationen einhalten, die im *SAP Global Information Classification and Handling Standard* dargelegt sind.

25.15.1 Papierdokumente

Vertrauliche SAP-Informationen:

- Müssen gesichert sein (z. B. in einem abgeschlossenen Aktenschrank, Büro oder Sicherungsbereich), wenn sie nicht genutzt werden
- Müssen in einem sicheren Container zerkleinert oder entsorgt werden, wenn sie weder genutzt noch archiviert werden; dies schließt auch vorläufige Arbeitsergebnisse ein, die Informationen enthalten, z. B. Memos oder Entwürfe
- Dürfen nur auf Papier ausgedruckt werden, wenn dies zur Ausübung der normalen Geschäftstätigkeiten notwendig ist

Vertrauliche und interne SAP-Informationen dürfen nicht unbeaufsichtigt auf Schreibtischen, Tischen oder Druckern liegen gelassen werden.

25.15.2 Bildschirme und Arbeitsplätze

SAP-Laptops und -Arbeitsstationen sind manuell zu sperren, wenn sie unbeaufsichtigt gelassen werden. (Mit ⊞ + L lässt sich zum Beispiel auf Windows-Computern der Bildschirm sperren.) Der Bildschirmschoner muss so konfiguriert werden, dass der Bildschirm nach einer Inaktivität von höchstens fünf Minuten automatisch gesperrt wird. Diese zeitabhängige Sperre von Geräten darf nicht deaktiviert werden.

Mobile Geräte, auf denen SAP-Informationen gespeichert sind oder die Zugriff auf andere SAP-Geräte oder -IT-Systeme ermöglichen könnten, müssen an einem sicheren Ort eingeschlossen werden, wenn sie nicht genutzt werden, beispielsweise in einem Aktenschrank, einer Kammer oder einer Schreibtischschublade.

25.16 Physische Sicherheit

Alle Mitarbeiter, externen Parteien und Besucher müssen die folgenden Anforderungen erfüllen:

- Zutrittskarten sind während des Aufenthalts auf SAP-Betriebsgelände deutlich sichtbar zu tragen.
- Karteninhaber dürfen ihre Zutrittskarten nicht verwenden, um anderen Personen Zugang zu gewähren.
- „Tailgating“ (unberechtigter Eintritt durch dichtes Nachfolgen) ist verboten.
- Karteninhaber müssen ihre Zutrittskarte an jedem Kartenlesegerät benutzen – egal, ob die Tür bzw. das Tor bereits geöffnet ist, wenn sie darauf zugehen.
- Der Verlust oder Diebstahl einer Zutrittskarte muss umgehend SAP Global Physical Security gemeldet werden.
- Alle Besucher müssen während ihres Aufenthalts auf dem SAP-Gelände und in abgesperrten Bereichen jederzeit von ihrem Gastgeber begleitet werden.
- Fotografieren, Filmen bzw. Aufnahmen auf dem SAP-Gelände sind ohne Genehmigung mit SAP Global Physical Security nicht gestattet.

- Wenn sperrige Gegenstände aus Gebäuden entfernt werden sollen, wird eine genehmigte Equipment Removal Form benötigt.
- Kombinationen, Codes oder Personal Identification Numbers (PINs), die für die physische Sicherheit genutzt werden, müssen alle sechs Monate geändert werden.
- Persönliche Gegenstände, Taschen, Brieftaschen, Schränke und von SAP zugewiesene Büroflächen dürfen bei hinreichendem Verdacht und im Rahmen der geltenden Gesetze und Vorschriften durchsucht werden.
- Waffen jeglicher Art sind auf dem gesamten SAP-Gelände verboten, sofern dies nicht dem geltenden lokalen Gesetz widerspricht.

25.17 Melden von Sicherheitsvorfällen

Alle tatsächlichen oder vermuteten Sicherheitsvorfälle müssen unverzüglich über das SAP-GSIM-Tool (Global Security Incident Management) im SAP Corporate Portal gemeldet werden.

Zu Sicherheitsvorfällen zählen unter anderem:

- Unberechtigter physischer Zugang zu einem Gebäude oder einem sicheren Ort, körperliche Gewalt, unmittelbar drohende Gefahr oder persönliche Sicherheitsfragen
- Nicht autorisierter Zugriff auf elektronische Systeme, die Eigentum von SAP sind oder von SAP betrieben werden, oder auf personenbezogene Informationen (Personally Identifiable Information, PII), die auf solchen Systemen gespeichert sind
- Böswillige Veränderung oder Vernichtung von Daten, Informationen oder Kommunikationen
- Nicht autorisiertes Abfangen oder Überwachen von Kommunikationen
- Jegliche vorsätzliche und unbefugte Zerstörung oder Beschädigung von IT-Systemen
- Die unsachgemäße Entsorgung von Unterlagen mit personenbezogenen Daten durch ein Team oder eine Einheit
- Verlust, Verlegung oder Diebstahl von Geräten, z. B. einer Arbeitsstation, eines Laptops, einer CD-ROM oder eines anderen Datenspeichers, auf denen sich SAP-Informationen befinden

25.18 Rückgabe von Assets

Bei Kündigung oder Auflösung des Vertragsverhältnisses müssen interne und externe Mitarbeiter alle Assets, die Eigentum von SAP sind, zurückgeben. Die vollständige Rückgabe aller Assets ist vom Vorgesetzten zu bestätigen. Zu diesen Assets zählen u. a. auch Laptops, mobile Geräte, Wechseldatenträger, Schlüssel, Zutrittskarten, Software sowie SAP-Informationen, -Dokumentationen und -Handbücher.