SAP GLOBAL SECURITY (SGS)

GLOBALER SICHERHEITSSTANDARD
Klassifizierung und Handhabung von Informationen

Versionsnummer: 2.0
Wirksamkeitsdatum: 26. Februar 2020
Dokumentklassifikation: INTERN

THE BEST RUN SAP®

DOKUMENTENBEZEICHNUNG

Dokumentumfang	SAP Global
Verantwortlich für das Dokument	Daniel Fryer Head of Security Policy, Standards and Risk Management
	Program Management and Communication
Überprüfungsturnus	Jährlich
Änderungsverzeichnis	Das vollständige Änderungsverzeichnis kann unter folgender Adresse angefordert werden: SAP_Security_Policy@exchange.sap.corp.
Versionsnummer	2.0
Wirksamkeitsdatum	26. Februar 2020
Status	Veröffentlicht

INHALTSVERZEICHNIS

1 EINFÜHRUNG

Informationen, definiert als bedeutungsvolle und zweckmäßige Daten, sind ein entscheidendes Asset der SAP. Wir müssen die Vertraulichkeit, Integrität und Verfügbarkeit unserer Informationen und der Informationen, die uns von unseren Kunden und Partnern anvertraut werden, gewährleisten. Ohne diese Schutzmaßnahmen können SAP-Informationen gefährdet sein, wodurch es zu einer Beeinträchtigung der Finanzen, der Wettbewerbsposition oder der Rechtslage unseres Unternehmens kommen kann.

Bei SAP-Informationen handelt es sich um 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-Informationen werden als **Vertraulich**, **Intern** oder **Öffentlich** klassifiziert. Für jede Klassifizierungsstufe gelten entsprechende Handhabungsanforderungen, für die von den jeweiligen Personen geeignete Schutzmaßnahmen und Sicherheitskontrollen durchzuführen sind.

2 ZWECK

Dieser Standard enthält die Kriterien und Anforderungen für die Klassifizierung und Handhabung von SAP-Informationen entsprechend ihrer Sensibilität, der damit verbundenen Risikostufe und den potenziellen Auswirkungen, die aus nicht autorisiertem oder unangemessenem Zugriff, der Nutzung, dem Verlust, der Änderung oder der Offenlegung entstehen können.

3 GELTUNGSBEREICH

Dieser Standard gilt für alle Geschäftseinheiten innerhalb der SAP, alle SAP-Mitarbeiter, alle externen Parteien, die Zugriff auf Informationen der SAP haben oder damit umgehen sowie für alle Informationen und Assets, die Eigentum der SAP sind oder von der SAP verwaltet werden.

Die Anforderungen in diesem Standard erstrecken sich auf alle Arten von SAP-Informationen, u. a. Papierdokumente, elektronische Daten, die in Systemen oder auf Medien gespeichert sind sowie Informationen, die in Cloud-Anwendungen von Drittanbietern gespeichert oder verarbeitet werden.

4 DEFINITIONEN

Assets (Vermögenswerte)	Etwas von materiellem oder immateriellem Wert; u. a. Personen, Informationen, Software, Hardware, Ausrüstung, Verfahren, Einrichtungen, ausgelagerte Dienstleistungen, geistiges Eigentum und Netzwerke
Verfügbarkeit	Sicherstellen von zeitnahem und verlässlichem Zugriff auf und die Nutzung von Informationen durch dazu befugte Instanzen
Autorisierte externe Mitarbeiter	Ein externer Mitarbeiter, der über das SAP External Workforce Center beschäftigt ist, an den Sicherheitsschulungen teilgenommen, die relevanten globalen Richtlinien zur Kenntnis genommen und eine entsprechende Vertraulichkeitsvereinbarung unterzeichnet hat
Geschäftseinheit	Jede SAP-Instanz, die ggf. speziell für ihre Geschäftsprozesse zusätzliche Sicherheitsanforderungen benötigt
Vertraulichkeit	Wahren von autorisierten Zugriffs- und Offenlegungsbeschränkungen für Informationen, 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-Laufwerke oder CDs) und Datenspeicher in mobilen Geräten.

Externe Partei	Eine dritte Partei, der Zugriff auf Informationen oder Assets von SAP erteilt wird. Hierbei kann es sich um externe Mitarbeiter, Auftragnehmer, Berater, Unterauftragsverarbeiter, Kunden, Lieferanten und Partner handeln.
Bestimmbare natürliche Person	Eine Person, die direkt oder indirekt mittels 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 Person sind, identifiziert werden kann
Informationen	Bedeutungsvolle und zweckmäßige Daten, die in unterschiedlicher Form, z. B. gedruckt, handschriftlich, mündlich oder elektronisch generiert oder gespeichert, vorliegen können
Informations-Asset	Ein Asset im Zusammenhang mit dem Zugriff auf Informationen, deren Verarbeitung, Nutzung oder Speicherung
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 vor unsachgemäßer Änderung oder Zerstörung von Informationen. Umfasst auch die Gewährleistung der Nachweisbarkeit und Authentizität von Informationen
Geistiges Eigentum	Patente, Urheberrechte, Geschäftsgeheimnisse, Marken und andere Rechte an geistigem oder gewerblichem Eigentum, die gesetzlich geschützt sind
Need to Know	Eine berechtigte und bestätigte Geschäftsanforderung für den Zugriff auf Informationen
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.
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.
Sicherheitskontrolle	Sicherheitsmaßnahme zur Risikominderung
Drittanbieter-Cloud-Anwendung	Eine Drittanbieter-Anwendung für Zwecke der Speicherung und Zusammenarbeit, die verwendet wird, um SAP-Geschäfte durchzuführen

5 ROLLEN UND ZUSTÄNDIGKEITEN

5.1 Informationseigentümer

Informationseigentümer (Information Owners) sind in der Regel Führungskräfte oder Manager mit der Befugnis, Informationen und Assets in ihrem jeweiligen Zuständigkeitsbereich zu erfassen, zu erstellen und zu pflegen.

Informationseigentümer sind verantwortlich für die:

- Auswahl der entsprechenden Klassifizierungsstufe für ihre Informationen
- Autorisierung, Prüfung und den Widerruf des Zugriffs auf ihre Informationen
- Gewährleistung, dass ggf. die entsprechende Vertraulichkeitsvereinbarung in Kraft ist
- Gewährleistung, dass Datenhaltung und -archivierung ordnungsgemäß verwaltet werden

Informationseigentümer sind außerdem dafür verantwortlich, die Vertraulichkeit der Informationen einzuschätzen und zu entscheiden, ob ein zusätzlicher (z. B. rechtlicher) Genehmigungsprozess vor ihrer Freigabe erforderlich ist.

5.2 Informationsnutzer

Informationsnutzer sind Einzelpersonen, die berechtigt sind, auf SAP-Informationen oder Informations-Assets zuzugreifen sowie diese zu ändern, zu löschen, zu erstellen und anderweitig zu handhaben. Dabei kann es sich auch um SAP-Mitarbeiter und externe Parteien handeln.

Alle Informationsnutzer sind zur Einhaltung dieses Standards verpflichtet. Personen, an die Informationen weitergeleitet oder weitergegeben werden, sind dafür verantwortlich, die entsprechenden Sicherheits- und Handhabungsanforderungen einzuhalten.

Personen, die Informationen erhalten, für die sie über keine Zugriffsberechtigung verfügen, müssen den entsprechenden Informationseigentümer oder den Absender informieren.

6 KLASSIFIZIERUNG VON INFORMATIONEN

Informationen müssen als **Vertraulich**, **Intern** oder **Öffentlich** klassifiziert werden, und angemessene Zugriffskontrollen sind einzuführen. Bei der Kombination von Informationen mit unterschiedlichen Sensibilitäten muss die restriktivste Klassifizierungsstufe des kombinierten Informations-Assets angewendet werden.

6.1 Vertrauliche Informationen

VERTRAULICH (CONFIDENTIAL)	
Klassifizierungs-kriterien	• **Hochsensible SAP-Informationen, die nur einer beschränkten Anzahl bestimmter Einzelpersonen zugänglich sind, bei denen ein definierter Zugriffsbedarf („Need to know“) vorliegt** • Im Falle einer nicht autorisierten Offenlegung, des Missbrauchs oder der Vernichtung können der Finanzlage, der Wettbewerbsposition oder der Rechtslage von SAP geschäftskritische oder erhebliche Schäden entstehen. • Folgende Informationen sind ebenfalls **vertraulich**: ✓ Informationen, die von SAP und Informationsnutzern aufgrund von Gesetzen, Vorschriften und/oder Verträgen geschützt werden müssen ✓ Informationen, die gemäß der *SAP Global Data Protection and Privacy Policy (SAP-Datenschutzrichtlinie)* als personenbezogene Daten gelten und den zusätzlichen Sicherheits- und Handhabungsanforderungen unterliegen, die in dieser Richtlinie definiert sind

Zugriffs-anforderungen für SAP-Mitarbeiter/ autorisierte externe Mitarbeiter	• Der Zugriff muss eingeschränkt und kontrolliert werden. • Informationseigentümer können einer beschränkten Anzahl bestimmter SAP-Mitarbeiter und/oder autorisierter externer Mitarbeiter Zugriff auf die Informationen gewähren, sofern bei diesen ein definierter Zugriffsbedarf („Need to know“) vorliegt. • Gesetzliche, behördliche und vertragliche Anforderungen müssen eingehalten werden.
Zugriffs-anforderungen für externe Parteien	• Der Zugriff muss eingeschränkt und kontrolliert werden. • Informationseigentümer können einer beschränkten Anzahl bestimmter externer Parteien (wie Kunden oder Partnern) Zugriff auf die Informationen gewähren, sofern bei diesen ein definierter Zugriffsbedarf („Need to know“) vorliegt. Mit den Einzelpersonen oder deren Organisation muss eine gültige Geheimhaltungsvereinbarung (Non-Disclosure Agreement, NDA) oder eine entsprechende Vertraulichkeitsvereinbarung geschlossen worden sein. • Gesetzliche, behördliche und vertragliche Anforderungen müssen eingehalten werden.
Leitfragen	Wenn die Antwort auf eine dieser Fragen „Ja“ lautet, sind die Informationen **Vertraulich**. 1. Handelt es sich um hochsensible Informationen, auf die nur von einer beschränkten Anzahl bestimmter Einzelpersonen zugegriffen werden darf, bei denen ein definierter Zugriffsbedarf („Need to know“) vorliegt? 2. Besteht aufgrund von Gesetzen, Vorschriften und/oder Verträgen eine Verpflichtung, die Informationen zu schützen? *3.* Enthalten die Informationen personenbezogene Daten gemäß der *SAP Data Protection and Privacy Policy*? 4. Würde die nicht genehmigte Offenlegung, der Missbrauch oder die Vernichtung der Informationen erhebliche Auswirkungen auf die Finanzen, die Wettbewerbsposition und/oder die Rechtslage der SAP haben?

6.2 Interne Informationen

INTERN (INTERNAL)	
Klassifizierungs-kriterien	• **Sensible SAP-Informationen, die SAP-Mitarbeitern und autorisierten externen Mitarbeitern zugänglich sind, wobei jeglicher anderweitige Zugriff jedoch eingeschränkt und kontrolliert werden muss** • Im Falle einer nicht autorisierten Offenlegung, des Missbrauchs oder der Vernichtung können der Finanzlage, der Wettbewerbsposition oder der Rechtslage von SAP mäßige oder geringfügige Schäden entstehen.
Zugriffs-anforderungen für SAP-Mitarbeiter/ autorisierte externe Mitarbeiter	• Der Zugriff ist unbeschränkt, sofern er zu geschäftlichen Zwecken der SAP erfolgt.
Zugriffs-anforderungen für externe Parteien	• Der Zugriff muss eingeschränkt und kontrolliert werden. • Informationseigentümer können externen Parteien (wie Kunden oder Partnern) Zugriff auf die Informationen gewähren. Mit den Einzelpersonen oder deren Organisation muss eine gültige Geheimhaltungsvereinbarung (Non-Disclosure Agreement, NDA) oder eine entsprechende Vertraulichkeitsvereinbarung geschlossen worden sein. • Gesetzliche, behördliche und vertragliche Anforderungen müssen eingehalten werden.
Leitfragen	Wenn die Antwort auf eine dieser Fragen „Ja“ lautet, sind die Informationen **Intern**. 1. Dürfen SAP-Mitarbeiter/autorisierte externe Mitarbeiter auf die Informationen zugreifen, der Zugriff durch andere externe Parteien muss jedoch eingeschränkt und kontrolliert werden? 2. Müssen die Informationen vor öffentlichem Zugriff geschützt werden, erfüllen jedoch nicht die Kriterien für die Klassifizierung „Vertraulich“?

	3. Würde die nicht genehmigte Offenlegung, der Missbrauch oder die Vernichtung der Informationen mäßige Auswirkungen auf die Finanzen, die Wettbewerbsposition und/oder die Rechtslage der SAP haben?

6.3 Öffentliche Informationen

ÖFFENTLICH (PUBLIC)	
Klassifizierungs-kriterien	• **SAP-Informationen, die keines besonderen Schutzes bedürfen und öffentlich verbreitet werden können** • Im Falle einer nicht autorisierten Offenlegung, des Missbrauchs oder der Vernichtung können der Finanzlage, der Wettbewerbsposition oder der Rechtslage von SAP unerhebliche oder keine Schäden entstehen. • Können offengelegt werden, ohne dass die Privatsphäre eines Einzelnen verletzt wird
Zugriffs-anforderungen für SAP-Mitarbeiter/ autorisierte externe Mitarbeiter	• Der Zugriff ist unbeschränkt.
Zugriffs-anforderungen für externe Parteien	• Der Zugriff ist unbeschränkt.

6.4 Besondere Aspekte

6.4.1 E-Mail

Der Inhalt und die Anhänge einer E-Mail bestimmen deren Klassifizierungsstufe. Beispielsweise veranlasst eine E-Mail-Adresse in einem Adressfeld allein keine Klassifizierung als **vertraulich**.

E-Mails mit **vertraulichen** Inhalten oder **vertraulichen** Anhängen müssen in Outlook als „vertraulich“ gekennzeichnet werden – und zwar unabhängig davon, ob sie an internes oder externes Publikum versendet werden.

6.4.2 Personenbezogene Daten

Personenbezogene Daten sind definiert als:

> *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.*

Mit anderen Worten sind personenbezogene Daten alle Informationen im Zusammenhang mit einer Einzelperson. Die Vertraulichkeit personenbezogener Daten ist abhängig von den Prozessen, in denen die Daten verwendet werden. Beispielsweise basiert die Vertraulichkeit eines Briefes oder einer E-Mail nicht allein auf einem Namen oder einer Adresse in der Anrede oder Überschrift, sondern auf dem gesamten Inhalt des Briefes oder der E-Mail.

Die spezifischen Anforderungen für die Definition, Verarbeitung und personenbezogene Daten sind in der *SAP Global Data Protection and Privacy Policy* geregelt.

7 POTENZIELLE AUSWIRKUNGEN

KLASSIFI-ZIERUNGS-STUFE	RISIKO-STUFE	AUSWIR-KUNGEN	**Negative Auswirkungen auf die Vertraulichkeit** *Nachteilige Auswirkungen der nicht autorisierten Offenlegung von Informationen*	**Negative Auswirkungen auf die Integrität** *Nachteilige Auswirkungen der nicht autorisierten Änderung oder Vernichtung von Informationen*	**Negative Auswirkungen auf die Verfügbarkeit** *Nachteilige Auswirkungen auf Störungen des Zugriffs oder der Nutzung von Informationen oder eines Informationssystems*
Öffentlich	Gering	Unwesentlich/ gering	Vernachlässigbar/keine	Vernachlässigbar/ keine	Vernachlässigbar/ keine
Intern	Mittel	Mäßig	Einige	Einige	Einige
Vertraulich	Hoch	Wesentlich/ geschäftskritisch	Erheblich	Erheblich	Erheblich

8 BEISPIELE

Diese Informationsbeispiele dienen als Orientierung für die Bestimmung der Klassifizierung von Informations-Assets. *Es handelt sich hierbei nicht um eine vollständige Liste aller SAP-Informationen oder Informations-Assets.* Informationseigentümer müssen die Klassifizierungskriterien verwenden, um den Informationen in ihrem Verantwortungsbereich die entsprechenden Klassifizierungsstufen zuzuweisen.

8.1 Beispiele für vertrauliche Informationen

VERTRAULICH (CONFIDENTIAL)	
Art von Information	**Beispiele**
SAP	• Hauptbuch • Dokumente des Integrationsprozesses • Produktdesign/funktionale Anforderungen • Datendateien, die Informationen enthalten, die durch Vorschriften/Bestimmungen geschützt sind • Marketingstrategien • Geschäftsbedingungen des Kunden • Entwürfe und abgeschlossene Service-Level-Vereinbarungen • Auditberichte von Dritten und interne Auditberichte • Interne Risikobewertungen und Ergebnisse • Ergebnisse von Schwachstellen-Scans • Berichte über Sicherheitsvorfälle und zugehörige Informationen • Audits, Pläne und Berichte in Bezug auf die Aufrechterhaltung des Geschäftsbetriebs und Disaster Recovery • Nicht öffentliche strategische Informationen (ausstehende Fusions-, Übernahme- oder Veräußerungspläne) • Nicht öffentliche finanzielle Informationen, wie tatsächliche oder prognostizierte Einnahmen und tatsächliche oder Eventualverbindlichkeiten • Notizen und/oder Protokolle zu Meetings von Führungskräften • Geplante Management- und organisatorische Änderungen • Nicht öffentliche Informationen in Bezug auf Unternehmensstreitfälle • Geschäftsgeheimnisse • Informationen zu Preisen, zur Entwicklung von Produkten und Dienstleistungen
Daten der Kreditkarten-industrie (Payment Card Industry, PCI)	• Primärkontonummer (Primary Account Number) • Name des Karteninhabers • Ablaufdatum • Servicecode • Full Track Data (Daten der Magnetstreifenspuren oder ähnliches) • CAV2/CVC2/CVV2/CID • PINs/PIN-Sperren
Personenbezogene Daten ***Es gelten die Anforderungen der SAP Data Protection and Privacy Policy.***	• Name • Anschrift oder E-Mail-Adresse • Telefonnummer • Sozialversicherungsnummer • Steueridentifikationsnummer • Geburtsdatum • Führerscheinnummer • Alter, Geschlecht, Familienstand • Identifikationsnummer, Symbol oder ein anderes Detail, die/das einer Person zugeordnet ist • Behinderung • Straftaten (einschließlich mutmaßlicher Straftaten) • Vorstrafen • Daten, mit denen eine natürlichen Person eindeutig identifiziert werden kann • Kunden-/Lieferantenlisten • Standortinformationen

Sensible personenbezogene Daten ***Es gelten die Anforderungen der SAP Data Protection and Privacy Policy.***	• Nationalität oder ethnische Herkunft • Glauben oder Religionszugehörigkeit • Politische Meinungen • Gewerkschaftsmitgliedschaft • Genetische Daten • Medizinische oder gesundheitsbezogene Informationen • Sexuelle Orientierung
Personalwesen	• Gehälter, Boni, Disziplinarmaßnahmen, Untersuchungen oder Hintergrundprüfungen • Informationen in Bezug auf Bonusprogramme • Leistungsauswahl einzelner Mitarbeiter • Nachfolgepläne für Führungskräfte • Mitarbeiterbeurteilungen • Werbeinformationen/-kennzahlen
Kunde/ Partner	• Kunden-/Lieferantenlisten • Alle Informationen, die auf der Grundlage einer Geheimhaltungsvereinbarung empfangen wurden • Daten, die von einem Kunden oder Partner als vertraulich definiert wurden
Nutzer-Authentifizierung	Benutzername oder ID in Verbindung mit: • Kennwörtern • Informationen für das Zurücksetzen eines Kennwortes oder zur Validierung der Identität eines Nutzers • Biometrischen Daten
Technologie	• Nicht-ABAP®-Quellcode • Informationen in Bezug auf nicht geschlossene Sicherheitslücken • Verschlüsselungscodes oder Passphrasen • Konfigurationseinstellungen oder -parameter für das Sicherheitssystem • Interne IP-Adressen

8.2 Beispiele für interne Informationen

INTERN (INTERNAL)	
Art von Information	**Beispiele**
SAP	• Leistungsbeschreibungen • Statusberichte • Richtlinien und Standards • Projektpläne
Kunde/ Partner	• Präsentationen oder Dokumentationen für Kunden und Partner, die nicht den Kriterien für Vertraulichkeit entsprechen, jedoch nicht veröffentlicht werden dürfen (u. a. kunden- oder partnerorientierte Dokumentation, die in Portale hochgeladen wird, auf die S-User zugreifen) • SAP-Hinweise • Status des Marketingkontakts
Personalwesen	• Mitarbeiterverzeichnis • Organigramme • Kennzahlen und Berichtsstatus für Mitarbeiter/Teams in operativen Prozessen • Mitarbeiterschulungen
Operative	• Verfahren • Wiki-Inhalte

8.3 Beispiele für öffentliche Informationen

ÖFFENTLICH (PUBLIC)	
Art von Information	**Beispiele**
Anwendungs-dokumentation	• SAP-Anwendungsbroschüren • SAP-Release-Informationen
Marketing/ Medien	• Marketing-Broschüren • Disclosure Statements von Kunden • Veröffentlichte Interviews mit den Nachrichtenmedien • Veröffentlichte Pressemitteilungen
Technologie	• ABAP®-Quellcode

9 HANDHABUNG VON INFORMATIONEN

Dieser Standard behandelt Handhabungsanforderungen aus Sicht der Informationssicherheit. Die Handhabung von Informationen kann auch durch bestimmte rechtliche, vertragliche oder behördliche Vorschriften vorgegeben sein. Zusätzlich zu den unten aufgeführten Handhabungsanforderungen müssen die folgenden SAP-Richtlinien eingehalten werden:

SAP Business Code of Conduct for Employees
SAP Global Data Protection and Privacy Policy
SAP Global Communications Policy

Die Handhabungsanforderungen, die für SAP-Mitarbeiter gelten, gelten ebenfalls für autorisierte externe Mitarbeiter.

	Handhabungsanforderungen	Vertraulich	Intern	Öffentlich
E-Mail an SAP-Mitarbeiter	In Outlook als „vertraulich“ markieren	X		
	Sicherstellen, dass der Informationseigentümer den Empfängern die Zugriffsberechtigung für die Inhalte und Anhänge erteilt hat	X		
	Ausschließlich von SAP bereitgestellte E-Mail-Services verwenden	X	X	
	Sicherstellen, dass keine E-Mail-Adressen versehentlich ausgewählt sind	X	X	
	Prüfen der Inhalte und Anhänge, um die Angemessenheit zu gewährleisten	X	X	X
E-Mail an externe Parteien	In Outlook als „vertraulich“ markieren	X		
	Geheimhaltungs- oder Vertraulichkeitsvereinbarung muss mit der externen Partei/Organisation geschlossen worden sein	X	X	
	Sicherstellen, dass der Informationseigentümer den Empfängern die Zugriffsberechtigung für die Inhalte und Anhänge erteilt hat	X	X	
	Ausschließlich von SAP bereitgestellte E-Mail-Services verwenden	X	X	
	Sicherstellen, dass keine E-Mail-Adressen versehentlich ausgewählt sind	X	X	
	Prüfen der Inhalte und Anhänge, um die Angemessenheit zu gewährleisten	X	X	X
Messaging-Anwendungen	Mitglieder von Gruppen oder Kanälen auf die Personen beschränken, bei denen bezüglich der besprochenen Informationen ein definierter Zugriffsbedarf („Need to know“) vorliegt	X		
	Mitglieder externer Parteien in Gruppen oder Kanälen auf Personen beschränken, die über Zugriffsberechtigungen für die besprochenen Informationen verfügen	X	X	
	Nur Messaging-Anwendungen verwenden, die von SAP IT bereitgestellt oder genehmigt wurden oder kundeninitiierte Messaging-Systeme, die den vertraglichen Verpflichtungen entsprechen	X	X	
Versand/Post an SAP-Mitarbeiter	Sicherstellen, dass der Informationseigentümer den Empfängern die Zugriffsberechtigung für die Informationen erteilt hat	X		
	Sicheres Verschließen der Verpackung	X		
	Zustellung direkt an den Empfänger oder einen autorisierten Vertreter. Nur dann die SAP-Hauspost nutzen, wenn eine direkte Zustellung nicht möglich ist	X		
	Verwenden der SAP-Hauspost oder direkte Zustellung an den Empfänger oder einen autorisierten Vertreter		X	
Versand/Post an externe Parteien	Zugangsbestätigung ist erforderlich	X		
	Geheimhaltungs- oder Vertraulichkeitsvereinbarung muss mit der externen Partei/Organisation geschlossen worden sein	X	X	
	Sicherstellen, dass der Informationseigentümer den Empfängern die Zugriffsberechtigung für die Informationen erteilt hat	X	X	
	Verpackung in versiegelten, sicheren und manipulationssicheren Umschlägen	X	X	
Papier/Ausdrucke	Nur ausdrucken, wenn es notwendig ist	X		
	Bei Nichtgebrauch sichern, sowohl innerhalb als auch außerhalb einer SAP-Einrichtung	X		
	Nicht unbeaufsichtigt auf Schreibtischen, Tischen oder Druckern liegen lassen	X	X	
	Bei Nichtgebrauch außerhalb einer SAP-Einrichtung sichern	X	X	
	Verwenden von dafür vorgesehenen Behältern für die sichere Entsorgung Wenn möglich, Aktenvernichter verwenden	X	X	

	Handhabungsanforderungen	Vertraulich	Intern	Öffentlich
Fax an SAP-Mitarbeiter	Sicherstellen, dass der Informationseigentümer den Empfängern die Zugriffsberechtigung für die Informationen erteilt hat	X		
	Sicherstellen, dass der Empfänger das Dokument erhalten hat	X		
	Die Originaldokumente dürfen nicht unbeaufsichtigt im Faxgerät verbleiben.	X	X	
	Ein Fax-Deckblatt des Unternehmens nutzen, auf dem die Klassifizierungsstufe angegeben ist	X	X	X
Fax an externe Parteien	Sicherstellen, dass der Informationseigentümer den Empfängern die Zugriffsberechtigung erteilt hat	X	X	
	Sicherstellen, dass der Empfänger das Dokument erhalten hat	X	X	
	Geheimhaltungs- oder Vertraulichkeitsvereinbarung muss mit der externen Partei/Organisation geschlossen worden sein	X	X	
	Die Originaldokumente dürfen nicht unbeaufsichtigt im Faxgerät verbleiben.	X	X	
	Ein Fax-Deckblatt des Unternehmens nutzen, auf dem die Klassifizierungsstufe angegeben ist	X	X	X
Kopieren/ Scannen	Gescannte Dokumente, die automatisch auf Netzlaufwerken gespeichert werden, müssen umgehend von der Person, die für das Scannen zuständig ist, gelöscht werden.	X		
	Originaldokumente und Kopien dürfen nicht unbeaufsichtigt im Kopierer verbleiben.	X	X	
Datenspeicherung	Der Zugriff auf Informationen muss auf autorisierte Personen mit Zugriffsbedarf („Need to know“) beschränkt sein.	X		
	Zugriff und Speicherung sind ausschließlich über Desktop-PCs, Laptops und mobile Geräte von SAP oder persönliche mobile Geräte, die durch eine Mobile-Device-Management-Lösung von SAP verwaltet werden, gestattet.	X	X	
Externe Cloud-Speicher	Der Zugriff auf Informationen muss auf autorisierte Personen mit Zugriffsbedarf („Need to know“) beschränkt sein.	X		
	Der Zugriff ist ausschließlich über Laptops, Desktop-PCs und mobile Geräte von SAP oder persönliche mobile Geräte, die durch eine Mobile-Device-Management-Lösung von SAP verwaltet werden, gestattet.	X	X	
	Nur in Lösungen gestattet, die von SAP IT genehmigt wurden	X	X	
Wechseldatenträger (tragbare Medien)	Müssen für den physischen Transport verschlüsselt sein. Die Informationen für die Entschlüsselung müssen über einen anderen Kommunikationskanal übertragen werden. Der Transport muss dokumentiert werden und rückverfolgbar sein.	X		
	Kundeninformationen dürfen nicht auf Wechseldatenträgern gespeichert werden.	X		
	Bei Nichtgebrauch sichern, sowohl innerhalb als auch außerhalb einer SAP-Einrichtung	X		
	Bei Nichtgebrauch außerhalb einer SAP-Einrichtung sichern	X	X	
	Müssen vor der Entsorgung entsprechend durch Überschreiben oder Entmagnetisierung bereinigt werden	X	X	
	Müssen für den physischen Transport gesichert sein	X	X	
Desktop-PCs und Laptops	Der Zugriff auf SAP-Informationen und deren Speicherung ist ausschließlich über Desktop-PCs oder Laptops von SAP gestattet.	X	X	
	Laptops und Desktop-PCs von SAP sind zu sperren, wenn sie unbeaufsichtigt gelassen werden. Mit ⊞ + L lässt sich zum Beispiel auf Windows-Computern der Bildschirm sperren.	X	X	X
Mobile Geräte	Der Zugriff auf SAP-Informationen und deren Speicherung ist ausschließlich über mobile Geräte von SAP oder persönliche mobile Geräte, die durch eine Mobile-Device-Management-Lösung von SAP verwaltet werden, gestattet.	X	X	
	Geräte, die für SAP-Geschäfte verwendet werden, dürfen nicht unbeaufsichtigt gelassen werden.	X	X	
Sprachkanäle	Sicherstellen, dass kein Unbefugter in der Nähe Gespräche verfolgen kann	X	X	
	Keine Informationen auf nicht gesicherten Anrufbeantwortern oder Voice-Mail-Systemen hinterlassen	X	X	

10 KENNZEICHNUNG DER INFORMATIONEN

10.1 Klassifizierungsstufen

Kennzeichnung ist die Praxis, Informationen mit einer Klassifizierungsstufe zu versehen, damit andere wissen, wie sie mit den Informationen richtig umgehen.

Informationseigentümer müssen alle **vertraulichen** und **internen** Informationen mit der entsprechenden Kennzeichnung versehen.

- In paginierten Dokumenten muss jede Seite des Dokuments gekennzeichnet werden, unabhängig vom Format (gedruckt, handschriftlich oder elektronisch).
- In nicht-paginierten Dokumenten (z. B. Webseiten) muss die Kennzeichnung neben dem Dokumenttitel oder oben auf der ersten Seite platziert werden.

Wenn möglich, sind Informationseigentümer angehalten, **öffentliche** Informationen zu kennzeichnen.

10.2 Optionale autorisierte Empfängergruppen

Es hat sich bewährt (optional), die autorisierten Empfängergruppen nach der Kennzeichnung **vertraulich** oder **intern** anzugeben. Dieses Vorgehen ermöglicht es dem Informationseigentümer:

- Die autorisierten Empfänger für **vertrauliche** Informationen anzugeben
- Bestimmten externen Parteien Zugriff auf **interne** Informationen zu gewähren

Der tatsächliche Wortlaut, der verwendet wird, um die autorisierten Empfängergruppen zu beschreiben, obliegt dem Informationseigentümer, wobei jedoch keine Eigennamen (d. h. Vor- oder Nachnamen) und personenbezogenen Daten verwendet werden dürfen.

Beispiele für diese optionalen Best Practices sind:

- Vertraulich: Nur für SAP-Vorstandsmitglieder
- Vertraulich: Nur für das SAP-Kundenprojekt XYZ
- Intern: SAP-Mitarbeiter und externe Mitarbeiter
- Intern: SAP-Kunden
- Intern: SAP-Partner

Zusätzlich bietet SAP IT eine Lösung in Microsoft Office an, die verwendet werden kann, um eine autorisierte Empfängergruppe zu identifizieren, indem eine vordefinierte Unterkennzeichnung an eine Klassifizierungsstufenkennzeichnung angehängt wird. (Diese Lösung steht möglicherweise nicht unter allen Betriebssystemen zur Verfügung.)

Die in diesem Standard definierten Handhabungs- und Zugriffsanforderungen für die einzelnen Klassifizierungsstufen gelten unabhängig vom angehängten Text. Der angehängte Text darf nur verwendet werden, um die autorisierten Empfängergruppen anzugeben und nicht, um andere Anforderungen zu ändern, hinzuzufügen oder zu löschen. Beispielsweise darf der angehängte Text nicht verwendet werden, um die Anforderung zu ändern, dass mit allen externen Parteien eine Geheimhaltungsvereinbarung oder eine entsprechende Vertraulichkeitsvereinbarung geschlossen worden sein muss.

Wenn der Informationsnutzer Informationen außerhalb der identifizierten autorisierten Empfängergruppe verbreiten möchte oder der angehängte Text unklar ist, muss der Informationseigentümer zwecks Autorisierung kontaktiert werden.

11 MELDEN VON SICHERHEITSVORFÄLLEN

Wenn **vertrauliche** oder **interne** Informationen jeglicher Art tatsächlich oder mutmaßlich verloren gegangen sind oder gegenüber nicht autorisierten Parteien offengelegt wurden oder es tatsächlich oder mutmaßlich zu einer nicht autorisierten Nutzung von SAP-Informations-Assets oder -Systemen gekommen ist, muss der Vorfall über das SAP-GSIM-Tool (Global Security Incident Management) im SAP Corporate Portal gemeldet werden.

12 STAATLICHE VERSCHLUSSSACHEN

Staatliche Verschlusssachen sind sämtliche Informationen, die entsprechend Gesetzen oder Vorschriften klassifiziert sind und zusätzlichen Schutz in Bezug auf Vertraulichkeit, Integrität oder Verfügbarkeit erfordern. Diese Informationen werden normalerweise mit verschiedenen Vertraulichkeitsstufen gekennzeichnet – beispielsweise **zugangsbeschränkt**, **vertraulich**, **geheim** oder **streng geheim**. Der Zugriff ist per Gesetz oder Vorschriften geregelt und offiziell autorisierten Personen vorbehalten. Unbefugter Zugriff oder unbefugte Offenlegung kann mit strafrechtlichen Sanktionen geahndet werden und das Ansehen von SAP schädigen. Eine formelle Sicherheitsüberprüfung ist eine obligatorische Voraussetzung für das Anzeigen, Verarbeiten oder Speichern von staatlichen Verschlusssachen oder den Zugriff darauf. Die Freigabe erfolgt in der Regel durch eine zuständige staatliche Stelle und wird gemeinsam mit einem beauftragten SAP Secrecy Officer durchgeführt.

Jeder, der mit Verschlusssachen oder Anfragen bezüglich zugehöriger Sicherheitsfreigaben in Berührung kommt (z. B. bei Kundenprojekten in stark regulierten und sicherheitsbewussten Branchen wie Verteidigung, Lieferanten für die Verteidigungsbranche, öffentlicher Dienst oder Kunden mit kritischen Infrastrukturkunden), muss sofort SAP Secrecy darüber informieren. Die E-Mail-Adresse lautet secrecy@sap.com.