Informationssicherheitsanforderungen für Lieferanten und Geschäftspartner

INHALTSVERZEICHNIS

1 GRUNDSÄTZE

1.1 EINLEITUNG

Informationen sind ein wesentlicher Vermögenswert der Swoboda Gruppe. Daher ist der Schutz und die Sicherung dieser Informationen von höchster Bedeutung für Swoboda. Das oberste Unternehmensziel, zentrale Geschäftsprozesse sowie die dafür benötigten Informationswerte und IT-Systeme effektiv zu schützen, wird durch die Schaffung global gültiger Sicherheitsstandards und die Integration von Informationssicherheit in interne Prozesse erreicht.

Lieferanten, deren Leistungen (in Form von Software, Hardware oder Dienstleistungen für Systeme) bei Swoboda eingesetzt werden, müssen die im Dokument beschriebenen Mindestanforderungen hinsichtlich der Qualität ihrer Arbeit und der Einhaltung von Maßnahmen zur Informationssicherheit erfüllen.

1.2 ZIELE

Ziel dieses Dokuments ist es, die sichere Integration von Dienstleistern und Lieferanten in den Geschäftsbetrieb zu gewährleisten. Dazu werden unter anderem die erforderlichen Regelungen zur Informationssicherheit als Grundlage für die Vertragsgestaltung mit Dritten beschrieben. Diese Regelungen zielen darauf ab, die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen der Swoboda Gruppe sowie deren Rechte und Interessen in Bezug auf Informationswerte zu schützen.

1.3 GELTUNGSBEREICH

Der Geltungsbereich betrifft verbundene Unternehmen und alle anderen Personen oder Unternehmen wie externe Partner oder Lieferanten, die Zugang zu Informationen der Swoboda Gruppe haben. Neben elektronisch gespeicherten Informationen zählen hierzu insbesondere auch Unterlagen und Gespräche.

1.4 DEFINITIONEN UND BENENNUNGEN

Auftragnehmer	Ein Auftragnehmer ist die Vertragspartei, die von einem Auftraggeber (Firma Swoboda) beauftragt wird, ein bestimmtes Geschäft oder eine Dienstleistung zu erledigen. Der Auftragnehmer übernimmt die Verantwortung für die Ausführung des Auftrags und muss dabei die im Vertrag festgelegten Bedingungen und Anforderungen erfüllen.
Auftraggeber	Ein Auftraggeber ist die Vertragspartei, die einem anderen (dem Auftragnehmer) im Rahmen eines Auftrags ein Geschäft zur Besorgung überträgt.
Informationseigentümer (engl. Data-Owner)	Der Data-Owner (Informationseigentümer) ist für einen bestimmten Teil der Daten innerhalb einer Organisation verantwortlich. Er hat volle Kontrolle über die Daten und stellt deren Schutz und Datenqualität sicher.

2 GRUNDLEGENDE SICHERHEITSANFORDERUNGEN

Fremdfirmen und deren Mitarbeiter (Auftragnehmer), die für die Swoboda Gruppe (Auftraggeber) tätig sind, verpflichten sich mit der Auftragsannahme:

- zur Umsetzung angemessener Sicherheitsmaßnahmen gemäß dem aktuellen Stand der Technik in Bezug auf ihre Leistungen für die Swoboda Gruppe. Grundlage hierfür sind: TISAX ISA Katalog, ISO 27001, EU-DSGVO, BSI IT-Grundschutz Kompendium und weitere einschlägige gesetzliche und branchenspezifische Anforderungen.
- zur Wahrung der Verschwiegenheit über interne Informationen des Auftraggebers und deren Mitarbeiter. Diese Verpflichtung besteht auch nach Beendigung der Vertragsverhältnisse fort.
- zum korrekten Umgang und zur Klassifizierung von digitalen und physischen Daten und Informationen gemäß dem Schutzklassenkonzept der Swoboda Gruppe.
- keine externen Geräte an das Firmennetzwerk anzuschließen. Ausnahmen bilden genehmigte VPN-Verbindungen oder das Gäste-WLAN.
- das Versenden, die Mitnahme oder das Kopieren von internen, vertraulichen und streng geheimen Dokumenten nur nach Freigabe durch den internen Informationseigentümer (Data-Owner) durchzuführen.
- die Nutzung von Smartphones, Videokameras oder sonstigen Bild- oder Tonaufzeichnungsgeräten nur nach vorheriger Erlaubnis des internen Ansprechpartners vorzunehmen.

3 PERSONAL

Der Auftragnehmer stellt sicher, dass

- dem Auftraggeber ein für Informationssicherheit verantwortlicher Ansprechpartner benannt wird.
- ausschließlich zuverlässiges und fachkundiges Personal für die Erfüllung des Auftrags sowie damit in Zusammenhang stehende Leistungen (z.B. Administration IT-Systeme des Auftraggebers, Durchführung internen Wartungsarbeiten) eingesetzt wird.
- seine Mitarbeiter, an den jährlichen IT-Sicherheits-, Informationssicherheits- und Datenschutzschulungen teilnehmen.
- relevante personelle Änderungen unverzüglich dem Auftraggeber mitgeteilt werden.
- die Mitarbeiter und – sofern zutreffend eingebundene Sub-Dienstleister / Unterauftragnehmer – nachweisbar auf ihre Verantwortung und Verpflichtungen in Bezug auf Informationssicherheit und Kundenvereinbarungen, insbesondere die Anforderungen des Auftraggebers, hingewiesen wurden.

Jeder, der im Namen des Auftragnehmers agiert, der entfernten oder lokalen Zugriff auf Systeme der Swoboda Gruppe haben muss, muss Informationen zu seiner Identität bereitstellen. Der Auftragnehmer stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall eintritt.

4 UMGANG MIT INFORMATIONSWERTEN

Bei der Speicherung, Übertragung, Verarbeitung, Archivierung, Vernichtung oder Löschung von Informationen und Datenträgern müssen die gesetzlichen Anforderungen berücksichtig werden sowie alle Schutzziele, wie Vertraulichkeit, Verfügbarkeit, Integrität, Verbindlichkeit, Verlässlichkeit und Privatsphäre, jederzeit gewährleistet sein.

4.1 KLASSIFIZIERUNG UND KENNZEICHNUNG VON INFORMATIONSWERTEN

Die Klassifizierung der Information wird durch den Informationseigentümer (Data-Owner) des Auftraggebers anhand des nachfolgenden Klassifizierungskriterien vorgegeben werden und sie muss über ihren gesamten Lebenszyklus hinweg aufrechterhalten und darf nur nach Freigabe durch den Informationseigentümer den Auftragsgebers verändert werden.

Folgende Stufen zur Klassifikation von Informationen hinsichtlich der Anforderungen an die Vertraulichkeit sind hierfür definiert:

Streng geheim (engl. Top Secret)
Unberechtigte Veröffentlichung oder Weitergabe solcher Informationen kann größere negative Folgen oder einschneidende Störungen von Geschäftsaktivitäten nach sich ziehen. Der Zugriff auf streng geheime Informationen muss auf eine geringe und namentlich genau festgelegte Anzahl von Personen begrenzt werden. Sparsamer Umgang mit dieser Klassifikation. Das Bekanntwerden der Informationen kann einen existenzgefährdenden Schaden verursachen. Streng geheime Informationen und Dokumente müssen mit ihrer Klassifizierungsstufe gekennzeichnet werden. Daten auf externen Medien und Datenträgern mit streng geheimen Inhalten müssen verschlüsselt werden.

Vertraulich (engl. Confidential)
Darunter fallen Informationen, deren Veröffentlichung der zukünftigen Entwicklung des Unternehmens erheblichen Schaden zufügen könnte (Wettbewerb, Finanzen, Rechtslage). Personenbezogene Daten müssen mindesten als vertraulich klassifiziert werden. Das Bekanntwerden der Informationen kann einen erheblichen Schaden verursachen und daher müssen diese Informationen nur einem begrenzten, berechtigten Personenkreis zugänglich gemacht werden. Vertrauliche Informationen und Dokumente müssen mit ihrer Klassifizierungsstufe gekennzeichnet werden. Vertrauliche Informationen, die an Parteien außerhalb Swoboda weitergegeben werden, müssen gemäß ihrer Klassifizierungsstufe gekennzeichnet sein. Daten auf externen Medien und Datenträgern mit vertraulichen Inhalten müssen verschlüsselt werden.

Intern (engl. Internal)
Für alle Mitarbeiter/Innen zugängliche Informationen, jedoch nicht für die Öffentlichkeit bestimmt. Weiterleitung nur an interne Mitarbeiter. Zugriff Externer darf nur mit Erlaubnis des Informationseigners erfolgen. Die Verwendung von Unternehmensinformationen in der Öffentlichkeit müssen zuvor mit den zuständigen Stellen abgestimmt werden. Das Bekanntwerden der Informationen kann einen geringen bis mittelgroßen Schaden verursachen. Interne Informationen und Dokumente müssen mit ihrer Klassifizierungsstufe gekennzeichnet werden.

Öffentlich (engl. Public)
Solche Informationen können für die allgemeine Öffentlichkeit zugelassen werden, daher sind keine Schutzmaßnahmen erforderlich. Das Bekanntwerden der Informationen hat keinen negativen Einfluss. Es ist empfohlen, öffentliche Informationen und öffentliche Dokumente mit ihrer Klassifizierungsstufe zu kennzeichnen. Bei der Weitergabe der öffentlichen Informationen und Dokumente nach extern ist eine Genehmigung der Auftraggeber erforderlich.

4.2 VERARBEITUNG VON PERSONENBEZOGENEN DATEN

Personenbezogene Daten dürfen nur auf Grundlage einer rechtlichen Basis erhoben und verarbeitet werden. Bei einer Auftragsverarbeitung müssen entsprechende vertragliche Vereinbarungen getroffen werden, die detaillierte Bestimmungen zu technischen und organisatorischen Schutzmaßnahmen enthalten.

4.3 NEED-TO-KNOW-PRINZIP UND LEAST-PRIVILEGE-PRINZIP

Grundsätzlich müssen die Berechtigungsvergabe und der Zugang zu Informationen nach dem Need-to-know-Prinzip und Least-Privilege-Prinzip erfolgen.

4.4 SCHUTZ VON DATENTRÄGERN

Vertrauliche, streng geheime und personenbezogene Informationen sind verschlüsselt zu speichern bzw. auf verschlüsselten Datenträgern aufzubewahren.

Nicht mehr benötigte Informationen müssen unverzüglich und sicher von den Datenträgern gelöscht werden.

4.5 SPEICHERUNG DER INFORMATIONEN IN EXTERNEN IT-DIENSTEN (CLOUD)

Die Verarbeitung von nicht-öffentlichen Informationen des Auftraggebers in externen IT-Diensten (Cloud) ist zulässig, sofern der Auftragnehmer sicherstellt, dass der externe Dienst ein gleichwertiges Sicherheitsniveau bietet.

4.6 ÜBERTRAGUNG DER INFORMATIONSWERTE

Interne, vertrauliche, streng geheime und personenbezogene Informationen ist bei der Übertragung über unsichere Netzwerke (z. B. Internet, Wi-Fi) stets zu verschlüsseln.

Vertrauliche, streng geheime und personenbezogene Informationen sollte bei der Übertragung über sichere Netzwerke (z. B. lokales, kabelgebundenes Netzwerk) verschlüsselt werden, falls technisch möglich ist.

4.7 BEREITSTELLUNG VON HARD- UND SOFTWARE

Wird dem Auftragnehmer vom Auftraggeber Hardware und Software bereitgestellt, so darf diese ausschließlich zur Speicherung und Verarbeitung von Informationen des Auftraggebers verwendet werden. Informationen, die nicht im Zusammenhang mit der Aufgabenerfüllung

stehen (z. B. private Informationen oder Informationen von anderen Kunden), dürfen nicht auf den bereitgestellten Geräten gespeichert oder verarbeitet werden. Der Auftraggeber behält sich das Recht vor, die Bereitstellung jederzeit zu beenden. Die Installation von Fremdsoftware auf durch Swoboda bereitgestellten Geräten bedarf einer Freigabe durch den Auftraggeber. Die Deaktivierung von Schutzmaßnahmen (z.B. Veränderung der Systemkonfigurationen, Deaktivierung des Malware-Schutzes oder lokaler Firewall, Installation der nicht durch Swoboda freigegebenen Software usw.) ist nicht zulässig.

4.8 RÜCKGABE UND LÖSCHUNG

Durch Swoboda bereitgestellte und nicht mehr benötigte Geräte und Datenträger sind unverzüglich, spätestens aber bei Vertragsende, beim Auftraggeber zurückzugeben. Auf Datenträgern des Auftragnehmers gespeicherte Informationen müssen bei Vertragsende vollständig an den Auftraggeber übergeben und anschließend sicher gelöscht werden. Vertraglich definierte und gesetzliche Aufbewahrungs- und Löschfristen sind hierbei einzuhalten.

5 SICHERHEIT VON IT-SYSTEMEN

5.1 IT-SICHERHEITSMAßNAHMEN

Sofern IT-Systeme des Auftragnehmers für die Erzeugung, Übertragung oder Speicherung von Daten für den Auftraggeber zum Einsatz kommen, gewährleistet der Auftragnehmer die Einhaltung von angemessenen IT-Sicherheitsmaßnahmen dieser Systeme gemäß aktuellem Stand der Technik, u.a.

- Berechtigungsmanagement, Rechte- und Rollenkonzepte, sichere Passwörter
- Patch-, Kapazitäts- und Schwachstellen-Management
- Datensicherung
- Kommunikationssicherheit
- Systemhärtung
- Kryptographie
- Malwareschutz
- Protokollierung
- Dokumentation

5.2 ZUGANG ZU IT-SYSTEMEN

Der Zugang zu IT-Systemen und Anwendungen muss ausschließlich durch personalisierte Zugangsdaten, d.h. eine Benutzerkennung und ein individuelles Passwort, erfolgen. Die Weitergabe der persönlichen Zugangsdaten an Dritte ist verboten. Die Zugangsdaten sind sicher aufzubewahren. Sammelaccount sind nicht erlaubt.

5.3 PASSWORT UND PIN-VORGABEN

Bei der Verwendung von Benutzerkonten (Standardbenutzer, technische Benutzer, privilegierte Benutzer, etc.) zur Anmeldung an IT-Systeme und Anwendungen oder bei der Verschlüsselung von Dateien ist die Passwortkomplexität wie folgt auszugestalten:

- Das Passwort muss mindestens 3 von 4 der Zeichentypen Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (z. B. !$%&) enthalten.
- Bei der Verwendung von Passwortmanager muss das Masterpasswort 4 von 4 Zeichentypen enthalten (Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (z.B. !$%&).
- Die Mindestlänge des Passworts muss 12 Zeichen betragen (auch für Office-Dokumente, ZIP-Archive usw.).
- Die Passwortmindestlänge der privilegierten Accounts und Service Accounts muss mindestens 15 Zeichen betragen.

Passwörter dürfen nicht leicht zu erraten sein. Hierbei sind insbesondere folgende Regeln mindestens organisatorisch anzuweisen:

- Keine Verwendung leicht ermittelbarer Daten aus dem persönlichen Umfeld (z. B. Name, Geburtsdatum, Firmenname oder Kostenstelle) oder Passwörtern, die im privaten Umfeld genutzt werden
- Keine Verwendung der User-ID als Bestandteil des Passworts.
- Vermeidung von aus Wörterbüchern stammenden Begriffen.
- Vermeidung von zyklischen Passwörtern (z. B. Wort01, Wort02).
- Keine Verwendung von Tastaturfolgen (z. B. asdfgh), Zahlenfolgen (z. B. 123456) oder Alphabetfolgen (z. B. abcdef).
- Die Anzahl der letzten Passwörter, die nicht verwendet werden dürfen (Passworthistorie), darf eine Anzahl von Zehn nicht unterschreiten.

Passwörter sind in den folgenden Fällen zu ändern:

- Standardpasswörter/Initialpasswörter von IT-Systemen und Anwendungen.
- Bei (Verdacht auf) Kenntnisnahme des Passwortes durch einen unberechtigten Dritten.
- Wenn ein bisheriger Berechtigter das Passwort nicht mehr für seine Aufgaben benötigt, sofern das Benutzerkonto nicht deaktiviert oder gelöscht wird (z.B. bei technischen Benutzerkonten).
- Passwörter aus Entwicklungs-, Test- und Integrationsumgebungen bei Inbetriebnahme des IT-Systems bzw. der Anwendung.

5.4 MULTI-FAKTOR-AUTHENTIFIZIERUNG

Die Multi-Faktor-Authentifizierung muss beim Zugang zu den IT-Systemen, bei denen vertrauliche, streng geheime oder personenbezogene Informationen verarbeitet und/oder gespeichert werden bzw. ein großes Risiko durch die Kompromittierung des Administrator- oder Benutzer-Accounts entstehen kann, implementiert werden.

Für den VPN-Zugang ist eine Multi-Faktor-Authentifizierung zwingend erforderlich.

6 SICHERE SOFTWAREENTWICKLUNG

Sofern der Auftragnehmer Software für den Auftraggeber entwickelt bzw. liefert, gewährleistet der Auftragnehmer

- eine sichere Test- und Entwicklungsumgebung (z.B. Zugriff auf Sourcecode, Versionskontrolle).
- die Einhaltung von Security Leitlinien und Best Practices zur sicheren Entwicklung (Security und Privacy by Design / by Default, Principle of Least Privilege, Segregation of Duties).
- Sicherheit in der Softwareentwicklungsmethodik (z.B. regelmäßige Überprüfungen, Codereviews).
- den Einsatz sicherer Repositorien.
- die Unternehmensdaten des Auftraggebers, welche im Rahmen von Softwareentwicklungsprojekten bei externen Dienstleistern gehostet werden, von den Daten anderer Kunden des Dienstleisters getrennt gespeichert, verarbeitet und transportiert werden.
- die Softwarepflege und -betreuung der Anwendung ausschließlich über die sicheren remote Zugänge des Auftraggebers durchzuführen.

7 DOKUMENTATION

Der Auftragnehmer hat eine ausführliche Dokumentation (insbesondere in Konzeptions- oder Entwicklungsphasen von Anwendungen und Systemen) zu erstellen und an den Auftraggeber auszuliefern. Der Auftragnehmer hat zu gewährleisten, dass

- der gesamte Entwicklungsprozess von der Anforderungs-, Designphase über die Entwicklung und Qualitätssicherung bis hin zur Überführung in die Produktion und anschließender Softwarewartung nur auf Basis einer dokumentierten und freigegebenen Spezifikation erfolgen darf.
- die Dokumentation so durchgeführt werden muss, dass ein Fachexperte mithilfe der Dokumentation den Programm-Code nachvollziehen und weiterentwickeln kann.
- Projekt-, Funktions- und Schnittstellendokumentationen müssen vollumfänglich erstellt und aktuell gehalten werden.
- eine Benutzer- und Administratorendokumentation angefertigt wird, die Hilfen zur Nutzung bzw. Administration der Anwendung gibt.

8 PHYSISCHE UND UMGEBUNGSBEZOGENE SICHERHEIT

Der Auftragnehmer muss sicherstellen, dass unbefugter Zutritt zu Räumen, Büros und Einrichtungen, in denen Informationen der Swoboda Gruppe verarbeitet werden, verhindert wird. Dies gilt auch für Produktions-, Anlieferungs- und Ladebereiche, über die unbefugte Personen Zugang erhalten könnten. Besonders wichtig ist der Schutz der Büroräume.

Alle zur Verfügung gestellten Informationswerte (z. B. Dokumente, Prototypen) und Geräte sind entsprechend ihrer Klassifizierung ordnungsgemäß zu behandeln und vor Einsichtnahme durch Dritte, Verlust und Diebstahl zu schützen.

Der Auftragnehmer ist verpflichtet, Richtlinien zu erstellen, die eine aufgeräumte Arbeitsumgebung sowie die Aktivierung von Bildschirmsperren bei Nichtbenutzung vorschreiben.

Sofern die Verarbeitung, Speicherung oder Aufbewahrung von Daten Bestandteil des Auftragsinhaltes ist, stellt der Auftragnehmer sicher, dass Vorkehrungen zur physischen Sicherheit und zum Zutrittsschutz getroffen werden. Dazu gehören u.a.

- Schutz gegen Feuer und Wasser
- Schutz vor bzw. Vermeidung von extremen Temperaturen (Klimaanlage)
- Notstromversorgung (USV, Notstromaggregat)
- Zutrittsschutz und Diebstahlschutz (Elektronische Zutrittskontrolle / Schließsystem, Alarmanlage, Videoüberwachung)

9 MELDEPFLICHTEN

Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die im Zusammenhang mit der vertraglichen Vereinbarung stehen und potenziell negative Auswirkungen auf materielle oder immaterielle Vermögenswerte der Swoboda Gruppe haben könnten, unverzüglich an Swoboda zu melden. Dazu gehören unter anderem:

- Verletzung von Gesetzen, vertraglichen Regelungen und Vorgaben
- IT- und Informationssicherheitsvorfälle (z. B. Industriespionage, Hackerangriffe oder Sicherheitslücken im Quellcode)
- Datenschutzvorfälle (z. B. Offenlegung personenbezogener Daten)
- Sonstige Risiken (z. B. Schwachstellen in IT-Systemen)

Im Falle eines Vorfalls muss der Auftragnehmer auf Anfrage Ressourcen zur Minderung, Meldung, Beweissicherung und Beseitigung des Vorfalls sowie den abschließenden Korrekturbericht bereitstellen.

10 ÜBERPRÜFUNG DER UMSETZUNG

Der Auftragnehmer willigt mit der Annahme des Auftrags ein,

- in angemessenem Umfang regelmäßige interne Prüfungen in Bezug auf die Einhaltung und Umsetzung von Sicherheitsmaßnahmen durchzuführen bzw. zu beauftragen.
- den Auftraggeber auf dessen Wunsch eine angemessene Überprüfung der Einhaltung und Umsetzung von Sicherheitsmaßnahmen im Rahmen von vor Ort Audits oder in Form angeforderter Nachweise (z.B. TISAX Label, ISO27001 Zertifikat) zu gestatten und dabei nach Kräften zu unterstützen, wobei vor Ort Audits grundsätzlich im Vorfeld angekündigt werden müssen.

11 KONTAKT

Für Fragen sowie zur Meldung von sicherheitsrelevanten Ereignissen, Sicherheits- oder Datenschutzvorfällen und sonstigen Risiken stehen Ihnen folgende Ansprechpartner zur Verfügung:

Information Security Officer: informationsecurity@swoboda.com
Datenschutzbeauftragter: datenschutzbeauftragter@swoboda.com

12 DOKUMENTHISTORIE

Datum	Beschreibung	Mitarbeiter
01.02.2025	Erstversion	Information Security Officer