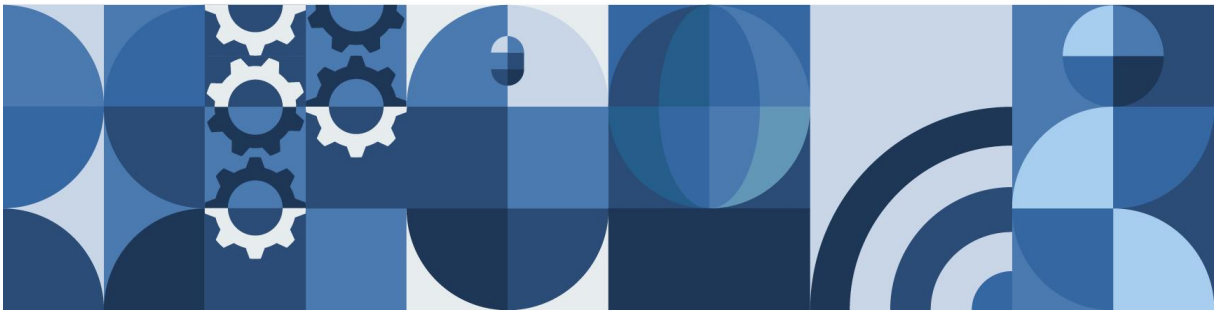
IT & DIGITALIZATION



Informationssicherheitsanforderungen für externe Partner

Version:	1.2
Datum der Version:	21.01.2025
Vertraulichkeitsstufe:	INTERNAL / BUSINESS

Inhaltsverzeichnis

Anmerkung: Aus Gründen der besseren Lesbarkeit wurde in diesem Dokument die männliche Form gewählt, sie bezieht sich auf Personen jeden Geschlechts.

1. Einleitung

1.1. Zweck

Diese Handlungsleitlinie beschreibt Mindestanforderungen an Informationssicherheit, die von Auftragnehmern des Auftraggebers – der VOSS Gruppe – beim Umgang mit VOSS Informationen und/oder IT-Geräten (z.B. Computern, Notebooks) eingehalten werden müssen. Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten und somit die Sicherheit unserer Geschäftsprozesse zu unterstützen.

Auftragnehmer im Sinne dieser Regelung sind Subunternehmer sowie Lieferanten für Dienstleistungen und Produkte.

In bestimmten Fällen können Kunden von VOSS ihrerseits strengere Vorgaben an den Informationsschutz einfordern die von betroffenen/involvierten Auftragnehmern zusätzlich einzuhalten sind.

1.2. Geltungsbereich

Diese Anweisungen gelten für alle Auftragnehmer, die schutzbedürftige Informationen für VOSS entsprechend vertraglichen Vereinbarungen verarbeiten oder diese von VOSS erhalten. Tochtergesellschaften und Niederlassungen von VOSS, sowie Gesellschaften, an denen VOSS beteiligt ist, sind von dieser Definition ausgeschlossen.

Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, sind nur temporär und nach Rücksprache mit den zuständigen Stellen und dem Auftraggeber VOSS zulässig und bedürfen einer Begründung.

Anforderungen in Ausschreibungen bzw. Verträgen gelten unabhängig von den Anforderungen dieser Richtlinie für den Auftragnehmer.

2. Allgemeines

Für die Wahrung der Informationssicherheit sind Regelungen zur Zusammenarbeit und Kommunikation zwischen VOSS und Auftragnehmern unerlässlich, insbesondere wenn firmenvertrauliche Informationen im Verlauf der Geschäftsbeziehung geteilt werden sollen.

VOSS hat sich daher freiwillig verpflichtet, das eigene Informationssicherheits-Managementsystem (ISMS) entsprechend den Informationssicherheitsstandards der ISO 27001 / VDA ISA (TISAX) zu betreiben.

3. Vorgaben zur Informationssicherheit

Der Auftragnehmer hat die folgenden Vorgaben zur Informationssicherheit in seinem Unternehmen umgesetzt:

3.1. Informationssicherheitsrichtlinien

Der Auftragnehmer hat Regelungen zur Informationssicherheit in seinem Unternehmen festgelegt und von der Leitung genehmigt. Den Beschäftigten wurden diese Regelungen bekanntgemacht.

3.2. Umgang mit Informationen

Informationen müssen nach ihrer Sensibilität klassifiziert und entsprechend geschützt werden. Der Zugang zu sensiblen Informationen muss kontrolliert und dokumentiert werden. Allen Beschäftigten, die mit Informationen umgehen, ist die Einstufung der Sensibilität und die davon abgeleiteten Regeln bekannt.

3.3. Identitätsmanagement

Die Registrierung, Deregistrierung und Zuteilung von Benutzerzugängen (z.B. Konten, Passwörter) ist ein formaler Prozess und wird dokumentiert. Der Umgang mit Passwörtern und Zugängen ist festgelegt und die Mitarbeiter sind zur Einhaltung dieser Vorgaben verpflichtet.

Eine Zuweisung von Zugriffsrechten erfolgt nach dem Need-To-Know-Prinzip. Die Erteilung von privilegierten Rechten geschieht restriktiv. Es wird gewährleistet, dass Benutzer nur auf die von ihrer Zugangsberechtigung umfassten Informationen zugreifen können. Es ist sichergestellt, dass die Anmeldeverfahren auf sicherem Wege geschehen und dem Stand der Technik entsprechen.

3.4. Remotearbeit

Sicherheitsmaßnahmen für die Arbeit außerhalb des Unternehmens sowie Maßnahmen zum Schutz von Information, auf die per Remotearbeit zugegriffen wird, sind umgesetzt.

3.5. Personalsicherheit & Training

In vertraglichen Vereinbarungen des Auftragnehmers mit bei ihm Beschäftigten und von ihm beauftragten Auftragnehmern (z.B. Subdienstleister) sind Geheimhaltungsverpflichtungen festgelegt. Mitarbeitende mit Zugang zu sensiblen Informationen/Tätigkeitsbereichen des Auftragnehmers wurden überprüft.

Beschäftigte werden regelmäßig zu Themen der Informationssicherheit, IT-Sicherheit und Datenschutz geschult.

3.6. Unterauftragnehmer

Für die Beauftragung von Subunternehmern durch den Auftragnehmer ist die Zustimmung von VOSS notwendig, sofern diese an für VOSS relevanten Prozessen beteiligt sind. Ist die Beauftragung von Subunternehmern vertraglich geregelt und hat VOSS der Beauftragung zugestimmt, hat der Auftragnehmer sicherzustellen, dass das hier beschriebene Informationssicherheitsniveau durch vertragliche Vereinbarungen sowie Überprüfungen auch beim Subunternehmen gewährleistet ist.

3.7. Assetmanagement

Alle Hard- und Softwarekomponenten müssen durch einen formalen Prozess über ihren gesamten Lebenszyklus hinweg verwaltet werden. Dies schließt die Beschaffung, Wartung und Betrieb, Außerdienststellung sowie Entsorgung ein. Zur Aufgabenerfüllung wird ausschließlich lizensierte Hard- und Software eingesetzt.

Der Auftragnehmer stellt sicher, dass die für Betriebssysteme und Anwendungen eingesetzten Softwarepakete aus sicheren Quellen stammen. Die regelmäßige Aktualisierung der eingesetzten Systeme und Anwendungen wird über einen gesteuerten Prozess gewährleistet.

Es sind Maßnahmen umgesetzt, die das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern (z.B. in Notebooks, Servern, externen Festplatten, USB-Sticks, etc.) verhindern. Es gibt Regeln und Verfahren zu sicherem Umgang, Entsorgung und Transport.

3.8. Endgeräteschutz

Der Auftragnehmer stellt sicher, dass die von ihm betriebenen Systeme und Hardware-Komponenten nach Stand der Technik gegen Schadsoftware, Manipulation oder Datenabfluss geschützt sind und kontinuierlich überwacht werden.

3.9. Kryptographie

Sensible Daten sind sowohl bei der Übertragung als auch bei der Speicherung verschlüsselt.

3.10. Sicherheitsvorfälle & Kontinuität

Verfahren zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen müssen vorhanden sein. Pläne zur Aufrechterhaltung des Geschäftsbetriebs im Falle eines Sicherheitsvorfalls müssen implementiert sein.

Es sind Verantwortlichkeiten und Verfahren zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen festgelegt. Genauso sind Pläne zur Aufrechterhaltung des Geschäftsbetriebs im Falle eines Sicherheitsvorfalls implementiert.

Alle Meldungen zu Informationssicherheitsereignissen haben schnellstmöglich an folgende Stelle zu erfolgen: **informationsecurity@voss.net**

3.11. Datensicherung

Der Auftragnehmer stellt sicher, dass Informationen jederzeit gegen Verlust geschützt sind und in einem angemessenen Zeitraum wiederhergestellt werden können.

3.12. Physische Sicherheit

Maßnahmen zur Sicherung der physischen Zugänge zu sensiblen Bereichen, Informationen und Systemen sind vorhanden. Eine Identifikation von Mitarbeitenden und Unternehmensfremden ist möglich (z.B. durch Mitarbeiterausweise o.ä.). Es ist geregelt und sichergestellt, dass nur berechtigte Personen in diese Bereiche gelangen können.

4. Zusätzliche Anforderungen an Auftragnehmer, die in der VOSS Infrastruktur arbeiten

Ein Auftragnehmer arbeitet in der VOSS-Infrastruktur, wenn:

- Clients (physische oder virtuelle Endgeräte) von VOSS zur Verfügung gestellt werden, oder
- die Anbindung über Remote-Access-Lösungen erfolgt mit Zugriff auf das VOSS interne Unternehmensnetzwerk (z.B. VPN), oder
- die Anbindung des Auftragnehmers direkt an das interne Unternehmensnetzwerk erfolgt (z.B. IPSec-Tunnel).

Für diese Auftragnehmer gelten die folgenden Anforderungen:

- Regelungen der jeweiligen Gesellschaft bezüglich des Mitbringens von VOSS-fremden IT-Geräten auf das Firmengelände oder in Sicherheitsbereiche müssen eingehalten werden.
- Die zur Verfügung gestellten Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen.
- Die Vorschriften des Herstellers zum Schutz der Geräte sind einzuhalten.
- Durch VOSS zur Verfügung gestellte Geräte (z.B. Notebooks) dürfen nur nach erfolgter Genehmigung vom Werksgelände mitgenommen werden.
- Auftragnehmer dürfen die Bereitstellung oder Installation von Hardware und Software nur über den für sie zuständigen Fachbereich von VOSS durchführen oder initiieren.
- Das Öffnen des IT-Gerätes und das Durchführen von Veränderungen an der Hardware (z. B. Ein-/Ausbau von Festplatten, Speicherbausteinen) sowie manuelle Veränderungen der Sicherheitseinstellungen (z. B. Browsereinstellungen) ist nur den zuständigen Stellen bei VOSS gestattet.
- Der Einsatz oder das nachträgliche Verändern der von VOSS zur Verfügung gestellten Programme ist nur zulässig, wenn dies von den zuständigen Stellen genehmigt wird.
- Auf den zur Verfügung gestellten IT-Geräten sind keine Daten von weiteren Kunden, die nicht zur VOSS Gruppe gehören, zu verarbeiten.