**Informationssicherheitsmanagement (ISMS) Richtlinie**

# Sicherheitsanforderungen an Externe

## Revisionsverfolgung

| Revision | Datum | Autor | Beschreibung der Änderung | Freigabe | Datum |
|---|---|---|---|---|---|
| 1.0 | 12.11.21 | ISB | Erstellung des Dokuments | Z | 15.11.2021 |
| | | | | | |

## Inhaltsverzeichnis

## 1. Ziel und Zweck

Um Werte der Flughafen Stuttgart GmbH (FSG) zu schützen, wird ein angemessenes Schutzniveau für die Vertraulichkeit, Verfügbarkeit und Integrität (Korrektheit) sowie deren Nachweisbarkeit in unseren Prozessen, Informationen und Systemen geschaffen.

Das erklärte Unternehmensziel, zentrale Geschäftsprozesse mitsamt dort benötigten Informationswerten und IT-Systemen effektiv zu schützen, wird durch die Schaffung global gültiger Sicherheitsstandards und die Integration von Informationssicherheit in interne Prozesse entsprochen. Dies gilt ebenso für interne als auch externe Mitarbeiter, Informationen und IT-Infrastruktur.

Der Schutz von Informationen, der korrekte Umgang mit IT-Equipment sowie Teile der Implementierung, Wartung und Betriebs der IT-Infrastruktur obliegen im Arbeitsalltag teilweise externen Unternehmen und deren Mitarbeitern. Aus diesem Grund werden im Rahmen dieser Richtlinie Vorgaben zum Umgang mit Informationen und IT-Equipment sowie IT spezifischen Vorgehensweisen, Prozessen und Anforderungen festgelegt.

Diese Richtlinie beinhaltet neben den Regeln der IT-Sicherheit auch wichtige Festlegungen für Mitarbeiter ohne IT-Arbeitsplatz. Die Regelungen reichen über den sicheren Betrieb elektronischer Geräte hinaus und umfassen generell den Umgang mit personenbezogenen Informationen und Geschäftsinformationen.

## 2. Grundlegende Sicherheitsanforderungen

Fremdfirmen und deren Mitarbeiter (Auftragnehmer), welche für die FSG (Auftraggeber) tätig sind, verpflichten sich mit der Auftragsannahme

- zur Umsetzung dem aktuellen **Stand der Technik** angemessener Sicherheitsmaßnahmen in Bezug auf deren Leistungen für die FSG. Grundlage hierfür sind die Handreichung zum aktuellen Stand der Technik des TeleTrust (https://www.teletrust.de/publikationen/broschueren/stand-der-technik/), ISO/IEC 27001, EU-DSGVO, BSI IT-Grundschutz Kompendium und weitere einschlägige gesetzliche und branchenspezifische Anforderungen (z.B. Informationssicherheitsanforderungen für kritische Infrastrukturen, die Energiewirtschaft, im Aviation-Sektor, IT-Sicherheitsgesetz etc.).
- die Wahrung der **Verschwiegenheit** über interne Informationen des Auftraggebers und deren Mitarbeiter. Diese Verpflichtung besteht auch nach Ende der Vertragsverhältnisse fort.
- zum **korrekten Umgang** und Klassifizierung von digitalen und physischen Daten und Informationen gemäß des Schutzklassenkonzepts der FSG.
- 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 und vertraulichen **Dokumenten** nur nach Freigabe mit dem internen Ansprechpartner durchzuführen.
- die **Nutzung** von Smartphones, Videokameras oder sonstigen Bild- oder Tonaufzeichnungen 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.

- 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.

## 4. Sicherheit von IT-Systemen

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.

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

## 5. Sichere Softwareentwicklung

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

- eine sichere 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 Repositories.
- 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.

## 6. 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.

## 7. Physische Sicherheit

Sofern die Verarbeitung / Speicherung / 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 (Elektronische Zutrittskontrolle/ Schließsystem, Alarmanlage, Videoüberwachung)

## 8. 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 zu gestatten und dabei nach Kräften zu unterstützen, wobei vor Ort Audits grundsätzlich im Vorfeld angekündet werden müssen.

## 9. Sicherheitsvorfälle

Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, welche im Kontext der vertraglichen Vereinbarung stehen und potentiell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte haben könnten, umgehend ohne Zeitverzug dem Vertragspartner zu melden. Dies könnte z.B. auch Industriespionage oder eine Sicherheitslücke im Source-Code sein.

Der Auftragnehmer muss im Falle eines Vorfalls auf Nachfrage Ressourcen zur Minderung, Meldung, Beweissicherung und Beseitigung des Vorfalles sowie den finalen Korrekturbericht bereitstellen.