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	15.11.21
2.0	17.04.25	FP1-2	Redaktionelle Überarbeitung; Neuer Anhang: Schutzklassen Kap. 1 Risikobasiertes Vorgehen	CE	16.05.2025

Inhaltsverzeichnis

1. Ziel und Zweck

Die Flughafen Stuttgart GmbH (FSG) hat das Ziel, ihre Unternehmenswerte und Informationen zu schützen. Hierzu muss ein angemessenes Schutzniveau für die Vertraulichkeit, Verfügbarkeit und Integrität (Korrektheit) unserer Informationen und Systeme geschaffen und in unseren Prozessen nachgewiesen werden. Bei der Umsetzung wird ein risikobasierter Ansatz gewählt, das heißt es müssen Maßnahmen implementiert werden, die geeignet sind, das identifizierte Risiko auf ein akzeptables Niveau zu reduzieren.

Das Ziel erreichen wir durch die Einführung und Einhaltung global gültiger Sicherheitsstandards und die Integration der Informationssicherheit in unsere Prozesse. Dies gilt gleichermaßen für interne als auch externe Mitarbeitende, Informationen und IT-Infrastruktur.

Die Verarbeitung von Informationen sowie Implementierung, Wartung und Betrieb von IT-Systemen und Infrastruktur können im Arbeitsalltag teilweise externen Unternehmen und deren Mitarbeitenden übertragen werden. Aus diesem Grund werden im Rahmen dieser Richtlinie Vorgaben zum Umgang mit Informationen und IT-Equipment sowie spezifische Vorgehensweisen, Prozesse und Anforderungen festgelegt.

Diese Richtlinie enthält neben Regeln der IT-Sicherheit auch wichtige Festlegungen für Mitarbeitende ohne IT-Arbeitsplatz. Sie gilt somit nicht nur für den sicheren Betrieb elektronischer Geräte, sondern umfasst generell den Umgang mit personenbezogenen und geschäftlichen Informationen.

2. Grundlegende Sicherheitsanforderungen

Fremdfirmen und deren Mitarbeitende (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 die für die FSG erbrachten Leistungen. Grundlage hierfür ist die Handreichung zum aktuellen Stand der Technik des TeleTrust [1].
  Maßgeblich für die FSG sind die Regelungen aus ISO/IEC 27001, EU-DSGVO, BSI IT-Grundschutz Kompendium und weitere einschlägige gesetzliche und branchen-spezifische Anforderungen (z.B. Informationssicherheitsanforderungen für kritische Infrastrukturen, die Energiewirtschaft, im Aviation-Sektor, IT-Sicherheitsgesetz etc.).
- zur Wahrung der **Verschwiegenheit** über interne Informationen des Auftraggebers und deren Mitarbeitende. Diese Verpflichtung besteht auch nach Ende der Vertragsverhältnisse fort.
- zum **korrekten Umgang** mit und Klassifizierung von digitalen und physischen Informationen gemäß des Schutzklassenkonzepts[2] der FSG. Zwischen Auftraggeber und Auftragnehmer ausgetauschte Informationen sind grundsätzlich als vertraulich zu behandeln, sofern die Informationen nicht ausdrücklich anders klassifiziert sind.
- keine **externen Geräte** an das Firmennetzwerk der FSG 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 durch die interne Ansprechperson durchzuführen.
- **Bild- oder Tonaufzeichnungen** mit Smartphones, Videokameras oder sonstigen Geräten nur nach vorheriger Erlaubnis der internen Ansprechperson vorzunehmen.

[1] https://www.teletrust.de/publikationen/broschueren/stand-der-technik
[2] Siehe Anhang: Schutzklassen der FSG

3. Personal

Der Auftragnehmer stellt sicher, dass

- dem Auftraggeber eine für Informationssicherheit verantwortliche Ansprechperson benannt wird.
- ausschließlich zuverlässiges und fachkundiges Personal für die Erfüllung des Auftrags sowie damit in Zusammenhang stehende Leistungen (z.B. Administration der IT-Systeme des Auftraggebers, Durchführung interner Wartungsarbeiten) eingesetzt wird.
- relevante personelle Änderungen unverzüglich dem Auftraggeber mitgeteilt werden.
- die Mitarbeitenden und – sofern zutreffend eingebundene Sub-Dienstleister / Unterauftragnehmer – nachweisbar auf ihre Verantwortung und Verpflichtungen in Bezug auf Informationssicherheit und die hierfür relevanten 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. beschränkter Zugriff auf Sourcecode, Versionskontrolle) und den Einsatz sicherer Repositories.
- 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).
- die Unternehmensdaten des Auftraggebers, welche im Rahmen von Softwareentwicklungsprojekten bei externen Dienstleistern gespeichert werden, von den Daten anderer Kunden des Dienstleisters getrennt gespeichert, verarbeitet und transportiert werden.
- die Softwarewartung und -betreuung der Anwendung ausschließlich über sichere 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 dem Auftraggeber zu übergeben. 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 (Software-)Wartung nur auf Basis einer dokumentierten und freigegebenen Spezifikation erfolgen darf.
- die Dokumentation so ausgeführt werden muss, dass ein Fachexperte mithilfe der Dokumentation die Funktion des Systems nachvollziehen und es erforderlichenfalls weiterentwickeln kann.
- Projekt-, Funktions- und Schnittstellendokumentationen müssen vollumfänglich erstellt und aktuell gehalten werden.
- eine Benutzer- und Administratorendokumentation angefertigt und übergeben wird.

7. Physische Sicherheit

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

- Schutz gegen Feuer, Wasser und andere schädliche Umwelteinflüsse
- Schutz vor bzw. Vermeidung von extremen Temperaturen (Klimaanlage)
- Stromversorgung (USV, Notstromaggregat)
- Zutrittsschutz (Elektronische Zutrittskontrolle oder Schließsystem, Besucherregelung, 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 potenziell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte haben könnten, umgehend dem Auftraggeber 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.

Anhang: Schutzklassen der FSG

Öffentlich
Personenkreis: Informationen der Klasse „Öffentlich“ dürfen ohne Einschränkungen frei weitergegeben werden, abgesehen von eventuellen urheberrechtlichen Aspekten. **Merkmale**: Die Weitergabe der Informationen führt zu keinen negativen Auswirkungen und verstößt gegen keine Gesetze. **Kennzeichnung**: nicht notwendig
Intern
Personenkreis: Informationen in dieser Klasse dürfen innerhalb der Organisation unbeschränkt und Partnern mit berechtigtem Interesse auch extern weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. **Merkmale**: Diese Informationen zeichnen sich durch eine Erhöhung der Sicherheitsrisiken im Schadensfall aus. **Kennzeichnung**: empfohlen
Vertraulich
Personenkreis: Informationen, die nur einem bestimmten Personenkreis wie beispielsweise Bereichen, Abteilungen, Projektteams (auch Externe) oder Prozessbeteiligten zur Verfügung stehen. **Merkmale**: Diese Informationen zeichnen sich im Schadensfall aus durch - Verstoß gegen gesetzliche Anforderungen, - finanzielle Schäden oder - Imageschäden. **Kennzeichnung**: notwendig mit dem Aufdruck „Vertraulich“
Streng Vertraulich
Personenkreis: „Streng Vertrauliche“ Informationen sind auf den Kreis der benannten Berechtigten beschränkt. Eine Weitergabe an andere (extern und intern) ist untersagt. **Merkmale**: Diese Informationen zeichnen sich im Schadensfall aus durch - hohe finanzielle Schäden - schwerwiegende Verstöße gegen gesetzliche Vorschriften - gesundheitliche oder wirtschaftliche Schäden für eine Person oder - nachhaltigen wirtschaftlichen Schaden für das Unternehmen. **Kennzeichnung**: notwendig mit dem Aufdruck „Streng Vertraulich“