

Anhang – Technische und organisatorische Maßnahmen (TOMs)

Summary

1.	Verlauf.....	3
2.	Einleitung dieses Dokuments.....	4
3.	Vertraulichkeit.....	5
3.1.	Physische Sicherheit.....	5
3.2.	Systemzugangskontrolle.....	5
3.3.	Sicherheitstests.....	5
3.4.	Verschlüsselung.....	5
4.	Integrität.....	6
4.1.	Änderungs- und Versionsmanagement.....	6
4.2.	Aufzeichnung und Überwachung.....	6
4.3.	Übertragungskontrolle.....	6
4.4.	Datenschutzmanagement.....	6
5.	Verfügbarkeit und Zuverlässigkeit.....	7
5.1.	Vorfallreaktionsmanagement.....	7
5.2.	Risikomanagement.....	7
5.3.	Geschäftskontinuität.....	7
5.4.	Bedrohungs- und Schwachstellenmanagement.....	7
5.5.	Audit.....	7

1. History

Datum	Autor	Zuständigkeit	Art der Änderung
05.01.2024	Johann Laqua	CISO	Erste Version des Dokuments

2. Einleitung dieses Dokuments

Dieses Dokument entspricht den Anforderungen gemäß Artikel 32 der DSGVO sowie den Artikeln 7 und 8 des Schweizer Bundesgesetzes über den Datenschutz (DSG).

Es beschreibt die technischen und organisatorischen Maßnahmen, die für alle Dienste und Kunden von Infomaniak gelten.

3. Vertraulichkeit

3.1. Physische Sicherheit

- Der physische Zugang zu den Unternehmensräumlichkeiten wird durch Systeme wie Ausweiskarten oder Gesichtserkennung kontrolliert.
- Der Zugang zu den Rechenzentren ist streng begrenzt.
- Die Überwachung erfolgt durch Videokameras, und bei einem Einbruch wird ein Alarm ausgelöst.
- Der Zugang ist personalisiert, dokumentiert und entsprechend den jeweiligen Rollen der Mitarbeitenden differenziert.
- Besucher dürfen sich nur in Begleitung eines Mitarbeitenden auf dem Gelände aufhalten.

3.2. Systemzugangskontrolle

- Eine Richtlinie zur Kontrolle des physischen und logischen Zugangs ist festgelegt und wird im gesamten Unternehmen kommuniziert.
- Es gilt eine Passwort-Richtlinie.
- Die Verwendung von Zwei-Faktor-Authentifizierung ist für alle Verbindungen zu den verschiedenen Diensten verpflichtend.
- Arbeitsstationen werden nach mehreren Minuten Inaktivität automatisch gesperrt.
- Es wurden Richtlinien zur Ordnung des Arbeitsplatzes („Clean Desk“) und zur Bildschirmdisziplin („Clear Screen“) eingeführt.
- Eine Richtlinie für mobiles Arbeiten und Telearbeit wurde ebenfalls festgelegt.
- Der gesamte Gerätepark ist durch Antivirensoftware geschützt.

3.3. Sicherheitstests

- Einsatz eines öffentlichen Bug-Bounty-Programms.
- Interne Sicherheitstests im Rahmen der Projektabläufe.
- Externe Sicherheitstests in Zusammenarbeit mit Cybersicherheitsunternehmen.

3.4. Verschlüsselung

- Alle Arbeitsstationen sind verschlüsselt.
- Remote-Verbindungen zum Firmennetzwerk sind per VPN verschlüsselt.
- Richtlinie zur kryptografischen Kontrolle und Verschlüsselung

4. Integrität

4.1. Änderungs- und Versionsmanagement

- Änderungsmanagement-Richtlinie wird angewendet und in die Dienste integriert.

4.2. Aufzeichnung und Überwachung

- Erfassung von Datenzugriffen und -änderungen.
- Zentralisierte Audit- und Sicherheitsprotokolle.
- Überprüfung der Vollständigkeit und Richtigkeit der Datenübertragung (End-to-End-Kontrolle).

4.3. Übertragungskontrolle

- Klassifizierung von Informationen nach Sicherheitsstufe.
- Jedem Informationselement wird entsprechend seiner Art ein Vertraulichkeitsgrad zugewiesen.
- Verpflichtende Nutzung verschlüsselter interner Tools für die Datenübertragung.

4.4. Datenschutzmanagement

- Datenschutzbeauftragte und ein Informationssicherheitsbeauftragter sind benannt.
- Eine Organisation für Datenschutz und Informationssicherheit wurde eingerichtet.
- Alle Mitarbeitenden werden für die Informationssicherheitskultur sensibilisiert.
- Die Mitarbeitenden werden für den Umgang mit personenbezogenen Daten sensibilisiert.
- Ein Verzeichnis der Verarbeitungstätigkeiten wird aktuell gehalten und Datenschutz-Folgenabschätzungen werden bei Bedarf durchgeführt.
- Verfahren zur Ausübung der Rechte betroffener Personen wurden eingerichtet.

5. Verfügbarkeit und Zuverlässigkeit

- Einsatz von Hardware- und Software-Firewalls.
- Systeme zur Erkennung von Eindringversuchen (Intrusion Detection Systems).
- Notfallhandbücher zur Datenwiederherstellung sowie zum Schutz vor unbeabsichtigtem Verlust oder Zerstörung.

5.1. Vorfallreaktionsmanagement

- Verfahren zur Reaktion auf Sicherheitsvorfälle.
- Krisenmanagementverfahren.
- Alle Rechenzentren sind nach ISO 27001 zertifiziert.
- Temperaturüberwachung der Anlagen in den Rechenzentren.

5.2. Risikomanagement

- Durchführung von Risikobewertungen zur Identifikation, Bewertung und Kategorisierung potenzieller Risiken für Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in der Organisation.
- Umsetzung eines Maßnahmenplans und geeigneter Kontrollmaßnahmen zur Bewältigung identifizierter Risiken.

5.3. Geschäftskontinuität

- Unterbrechungsfreie Stromversorgung (USV) und Notstromgeneratoren zur Sicherstellung der Dienstverfügbarkeit bei Stromausfällen.
- Redundanz in kritischen Systemen zur Minimierung von Single Points of Failure.
- Maßnahmen zur Abwehr von DDoS-Angriffen zum Erhalt der Verfügbarkeit der verwalteten Dienste.
- Regelmäßige Tests der Datensicherungen.
- Periodische Wiederherstellungsübungen.
- Ein Business Continuity Plan (BCP) ist definiert, wird verwaltet und von den Produktionsteams überwacht.

5.4. Bedrohungs- und Schwachstellenmanagement

- Regelmäßige Scans unserer Infrastruktur zur Erkennung von Schwachstellen.
- Systemaktualisierungen durch die zuständigen Produktionsteams.
- Zusammenarbeit mit Partnern zur Erkennung externer Bedrohungen.
- Technologische Überwachung unserer Assets und internen Tools.

5.5. Audit

- Interne Audits durch qualifizierte Berater für die nach ISO 27001 zertifizierten Bereiche.
- Jährliche externe Audits durch ISO 27001-Zertifizierungsstellen.

- Ad-hoc-Technikaudits durch qualifizierte Experten für Informationssysteme nach Bedarf.