Sicherheitsplan

Infomaniak Network

Inhalt

1. Verlauf

Datum	Verfasser*in	Funktion	Art der Änderung
13.05.2025	Johann Laqua	RSSI	Wechsel des Firmenlogos, Aktualisierung der Kapitel zur physischen Sicherheit, Hinzufügung des Kapitels für Definitionen
19.04.2024	Johann Laqua	RSSI	Fertigstellung des Dokuments zur Erstveröffentlichung
14.02.2024	Johann Laqua	RSSI	Erste Fassung des Dokuments

2. Über dieses Dokument

In diesem Dokument soll der Sicherheitsplan von Infomaniak Network SA dargelegt werden.

3. Einleitung

3.1. Zweck des Dokuments

In diesem Dokument ist unser Sicherheitsplan (PAS) dargelegt, der Verträgen mit unserer Kundschaft beigefügt werden kann. Dieser Plan umfasst die Verpflichtungen, denen Infomaniak Network zur Erfüllung der vertraglichen Anforderungen in Bezug auf die Sicherheit von Informationssystemen (SSI) nachkommt. Durch diese Anforderungen:

- soll der Schutz der Ressourcen der bei der Erbringung der vertraglich vereinbarten Dienstleistungen eingesetzten Informationssysteme gewährleistet werden;
- sollen unsere Kunden vor Schäden geschützt werden, die sich aus der Nichtverfügbarkeit dieser Ressourcen sowie aus einer Verletzung ihrer Integrität oder Vertraulichkeit ergeben können.

In unserem Sicherheitsplan (PAS) sind die verschiedenen sicherheitsspezifischen Bestimmungen, einschliesslich unserer physischen, organisatorischen, verfahrenstechnischen und technischen Massnahmen, dargelegt.

3.2. Anwendungsbereich

Dieses Dokument bezieht sich auf die von den Teams von Infomaniak Network verwalteten Dienste sowie deren Tätigkeiten.

3.3. Entwicklung

Jegliche Änderungen am Sicherheitsplan (PAS) ziehen eine neue Fassung dieses Dokuments nach sich. Vorgenommene Änderungen werden in der Versionshistorie des Dokuments erfasst und datiert.

Der Sicherheitsplan (PAS) wird mindestens einmal jährlich von den für Compliance und die Sicherheit der Informationssysteme zuständigen Mitarbeitenden überprüft und von der Geschäftsleitung genehmigt.

3.4. Begriffsbestimmungen

RSSI: Verantwortlicher für die Sicherheit von Informationssystemen
ISO: Internationale Organisation für Normung
EBIOS: Bedarfsäusserung und Ermittlung von Sicherheitszielen
Red Team: Sicherheitsteam mit Schwerpunkt auf Übungen und Tests der offensiven Sicherheit mit Personen aus verschiedenen Abteilungen.
ASDPO: Vereinigung Schweizerischer Datenschutzbeauftragter
NCSC: National Cyber Security Centre
CERT: Computer Emergency Response Team
HR: Humanressourcen

HTTPS: Hypertext Transfer Protocol Secure
SSL: Secure Sockets Layer
IMAPS: Internet Message Access Protocol Secure
SMTPS: Simple Mail Transfer Protocol Secure
POP3S: Post Office Protocol 3 Secure
IDS: Intrusion Detection System
DDoS: Distributed Denial of Service
CVE: Common Vulnerabilities and Exposures
BCP: Business Continuity Plan
RPO: Recovery Point Objective
RTO: Recovery Time Objective
DSG: Bundesgesetz über den Datenschutz
DSGVO: Datenschutz-Grundverordnung

4. Bewährte Praktiken

Die Sicherheit von Infomaniak Network wird von einem Sicherheitsausschuss sowie einem Compliance-Team gemäss den Standards der ISO-Norm 27001 für das gesamte Unternehmen überwacht. Infomaniak Network ist für folgende Bereiche und Tätigkeiten nach ISO 27001:2022 zertifiziert:

Entwicklung und Bereitstellung von Cloud-Infrastrukturen, Webdiensten, Anwendungen, Kundensupport sowie der Wartung von Datacentern.

5. Risikomanagement

Infomaniak Network hat eine schriftliche Bewertung der Risiken vorgenommen, die den gesamten Anwendungsbereich des Sicherheitsplans abdeckt und auf einer dokumentierten Methodik beruht, die die Reproduzierbarkeit und Vergleichbarkeit des Vorgehens gewährleistet.

Dieser Risikobewertungsprozess umfasst eine Risikoanalyse, Risikomanagement und Pläne zur Risikominderung, die in konkrete Massnahmen und Projekte münden.

Darüber hinaus stützt sich Infomaniak Network auf allgemein anerkannte Methoden wie EBIOS RM, um Risiken im Rahmen seines Managementsystems für Informationssicherheit (SMSI) zu steuern.

6. Richtlinie zu Informationssicherheit

Infomaniak Network hat eine Richtlinie zu Sicherheit verabschiedet, die unter folgender Adresse abrufbar ist: https://www.infomaniak.com/documents/politique_SI_EE_de.pdf

Darin sind unsere Verpflichtungen und Ziele im Bereich der Informationssicherheit klar dargelegt.

7. Organisation der Informationssicherheit

Um unseren Ansatz für die Sicherheit von Informationssystemen (SSI) zu strukturieren, haben wir mehrere komplementäre Instrumente eingeführt, d. h. ein spezifisches Organigramm für SSI, eine Politik für die Sicherheit von Informationssystemen (PSSI) sowie ein Managementsystem für Informationssicherheit (SMSI). Diese Elemente sind von entscheidender Bedeutung, um die strikte und kohärente Anwendung unserer Sicherheitsverfahren zu gewährleisten.

7.1. Aufgaben und Verantwortlichkeiten

Die Verantwortlichkeiten im Sicherheitsbereich wurden festgelegt und zugeteilt.

Infomaniak Network hat einen Chief Information Security Officer (CISO) ernannt. Diese Person überwacht alle technischen und organisatorischen Maßnahmen, die im Rahmen unserer umfassenden Informationssicherheitsstrategie umgesetzt werden.

Ein Sicherheitsausschuss, bestehend aus den Leitern der verschiedenen Abteilungen und technischen Teams des Unternehmens, trifft sich wöchentlich zu SOC (Security Operations Center) -Meetings, um Themen im Zusammenhang mit der Informationssicherheit zu besprechen.

Unter der Aufsicht des CISO führt ein Red Team Sicherheitsprüfungen an Produkten und Social-Engineering-Tests bei den Mitarbeitern des Unternehmens durch.

7.2. Governance

Auf strategischer und operativer Ebene wird ein spezielles Governance-Team eingerichtet.

Dieses Team tritt regelmässig zusammen, um Sachverhalte im Zusammenhang mit der Sicherheit von Informationssystemen zu überwachen. Die Protokolle dieser Sitzungen werden sicher gespeichert.

7.3. Umgang mit Stellen und Behörden

Infomaniak Network ist Mitglied von Berufsverbänden (ASDPO) und unterhält Beziehungen zu Behörden (NCSC und Cyber Security Hub) für Entwicklungen im Bereich der Informationssicherheit.

7.4. Überwachung und Sicherheit

Im Rahmen der Tätigkeit erfolgt eine Überwachung der technischen und rechtlichen Sicherheit. Diese
ermöglicht, Risiken vorzubeugen, die speziell mit den Tätigkeiten von Infomaniak Network verbunden sind.

Infomaniak Network stützt sich auf eine Partnerschaft mit einem auf Cybersicherheit spezialisierten Unternehmen, um das Darkweb im Hinblick auf sensible Vermögenswerte zu überwachen, die unter seine Verantwortung fallen.

8. Personalsicherheit

8.1. Rekrutierung

Unsere HR-Abteilung wendet für alle neu einzustellenden Bewerber*innen ein Rekrutierungsverfahren mit Sicherheitsmassnahmen an, die der Einstufung jedes Mitarbeitenden und den identifizierten Risiken angemessen sind.

Folgende Überprüfungen werden durchgeführt:

- Überprüfung der Identität der Bewerber*innen
- Überprüfung der Kompetenzen der Stelle
- Überprüfung der Referenzen der Bewerber*innen
- Überprüfung des Strafregisters
- Umfassende Zuverlässigkeitsüberprüfung bei Bewerber*innen mit hoher Sicherheitsstufe

8.2. Umgang mit vertraulichen Daten

In den Arbeitsverträgen sind die Verantwortlichkeiten der Mitarbeitenden für Informationssicherheit klar geregelt.

Gemäss einer Geheimhaltungsklausel in den allgemeinen Bedingungen des Arbeitsvertrags sind die Mitarbeitenden verpflichtet, die Vertraulichkeit sensibler und privater Daten, auf die sie im Rahmen ihrer Tätigkeit bei Infomaniak Zugriff haben, strikt zu wahren. Jegliche Verletzungen ziehen Folgen für den jeweiligen Betroffenen nach sich.

Zudem wurde ein formelles Disziplinarverfahren eingerichtet und allen Mitarbeitenden sowie weiteren Anspruchsgruppen kommuniziert. In diesem Verfahren sind angemessene Sanktionen für jegliche Personen vorgesehen, die gegen die Politik für Informationssicherheit verstossen haben.

8.3. Schärfung des Sicherheitsbewusstseins

Wir führen Sicherheitsüberprüfungen durch, um die Konformität der Arbeitsstationen zu gewährleisten; gleichzeitig schärfen wir das Bewusstsein unserer Kolleginnen und Kollegen für die Risiken für die Sicherheit von Informationssystemen (SSI) und unsere Verfahren für die physische und logische Sicherheit.

Bei diesen Überprüfungen legen wir auch wichtige Dokumente wie unsere Politik für Informationssicherheit (PSI) und unsere Allgemeinen Sicherheitsrichtlinien vor.

Wir erarbeiten jährlich ein Sensibilisierungsprogramm mit diversen Bewertungstools zu verschiedenen Themen im Zusammenhang mit Sicherheit und Cybersicherheit. Dazu gehören unter anderem Phishing- und Social-Engineering-Kampagnen.

Die Mitarbeitenden erhalten mehrere E-Mail-Mitteilungen, um ihr Bewusstsein für Risiken für Informationssicherheit, den Datenschutz, Cyber-Risiken sowie Aktualisierungen unseres Managementsystems für Informationssicherheit zu schärfen.

8.4. IT-Charta

Infomaniak Network verfügt über allgemeine Sicherheitsrichtlinien, die einer IT-Charta gleichzusetzen sind, regelmässig aktualisiert und allen Mitarbeitenden unseres Unternehmens kommuniziert werden.

Alle Mitarbeitenden verpflichten sich bei Einstellung an Eides statt, diese einzuhalten; andernfalls drohen Disziplinarmassnahmen.

8.5. Kompetenzen und Schulungen

Die Personalabteilung führt jedes Jahr im Rahmen von Einzelgesprächen eine Mitarbeiterbefragung durch, um ihren Bedarf an Weiterbildungen zu ermitteln. Anschliessend wird ein jährliches Schulungsprogramm erstellt, in dem die erforderlichen Schulungen festgeschrieben sind, um:

- Kompetenzlücken von Mitarbeitenden, Teams oder Fachbereichen zu beseitigen;
- dem Bedarf an der fortwährenden Entwicklung von Kompetenzen gerecht zu werden.

Die angebotenen Schulungen können intern oder von externen Anbietern durchgeführt werden.

Um die Kompetenzen unserer Mitarbeitenden zu stärken, bieten Delegierte oder Expert*innen für Cybersicherheit das ganze Jahr über verschiedene technische Schulungen an, und es werden vierteljährliche Berichte und Statistiken über Schwachstellen erstellt, die unsere Systeme beeinträchtigen könnten.

8.6. Vertragsende

Es wurde ein Austritts- bzw. Kündigungsverfahren eingerichtet und allen betroffenen Verantwortlichen im Unternehmen kommuniziert. Mit diesem Vorgehen soll sichergestellt werden, dass der jeweilige Mitarbeitende weder physisch noch softwaregestützt auf das betriebliche Informationssystem zugreifen kann.

9. Verwaltung der Vermögenswerte

9.1. Bestand

Infomaniak Network erstellt Verzeichnisse wichtiger Vermögenswerte und unterstützender Güter. Diese sind in unserem Managementsystem für Informationssicherheit (SMSI) sowie in unseren Risikobewertungen dargelegt.

Wir überprüfen diese Vermögenswerte jährlich durch das SMSI und aktualisieren sie in automatisierten Prozessen gemäss den Anforderungen der verschiedenen internen Teams.

9.2. Software-Lizenzen

Infomaniak Network ist entschlossen, innerhalb seiner internen Teams die Nutzung gültiger Lizenzen für Software von Drittanbietern zu gewährleisten, und ergreift die erforderlichen Massnahmen zum Schutz der Rechte des geistigen Eigentums.

9.3. Identifikation und Einstufung von Vermögenswerten

Vermögenswerte werden segmentiert und durch eine von den internen Teams erstellte Nomenklatur und Namenskonvention eindeutig identifiziert. Es erfolgen kontinuierliche und jährliche Kontrollen, um die Rechtmässigkeit der Zugriffe, die Beschränkung unbefugter Zugriffe und die Zuverlässigkeit des Bestands zu gewährleisten.

Daten werden entsprechend den Informationssicherheitsbedürfnissen der Organisation eingestuft, wobei die Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen sowie die wichtigsten Anliegen der Anspruchsgruppen berücksichtigt werden.

9.4. Aktualisierungen, Virenschutz und Verschlüsselung von Trägern

Der Beauftragte für die Sicherheit von Informationssystemen (RSSI) überwacht den zentralen Schutz der Vermögenswerte des Unternehmens, einschliesslich der Arbeitsstationen der Mitarbeitenden, vor Viren und Malware. Die Abwehrstrategie gegen diese Bedrohungen wird durch eine entsprechende Schulung der Nutzer*innen verstärkt.

Die Sicherheit der internen und entfernbaren Speichermedien wird durch einen konfigurierten und überwachten Verschlüsselungsprozess gewährleistet.

Zur Überprüfung der Konformität und des Schutzes der Vermögenswerte werden regelmässig wesentliche Leistungsindikatoren (KPI) erfasst.

9.5. Telearbeit

Um die Informationssicherheit bei Telearbeit zu gewährleisten, wurden verschiedene Vorkehrungen getroffen. So wurden spezielle Telearbeitsrichtlinien erarbeitet und den Mitarbeitenden kommuniziert. Es ist zwingend erforderlich, ein sicheres virtuelles privates Netzwerk (VPN) zu verwenden, um eine externe Verbindung zu den Ressourcen der Organisation herzustellen.

Zudem ist die Verwendung privater Geräte ("Bring Your Own Device" bzw. BYOD) in diesem Zusammenhang nicht gestattet.

9.6. Verwaltung von Wechseldatenträgern und entfernbaren Geräten

Es wurden Richtlinien für die Verwendung von Wechseldatenträgern erstellt und verbreitet, die dem Personal bekannt sind. Diese Anweisungen umfassen strenge Regeln für deren Verwendung, um potenzielle Risiken zu minimieren, und Empfehlungen, um deren Schutz zu gewährleisten.

So kann es erforderlich sein, Wechseldatenträger mit vertraulichen oder kritischen Daten zu verschlüsseln oder ihre Verwendung auf bestimmte besondere Umstände zu beschränken.

9.7. Entsorgung

Es wurde eine Politik für das Recycling von Hardware und die Stilllegung von Vermögenswerten festgelegt und umgesetzt, um sensible Vermögenswerte des Unternehmens zu verwalten.

Ziel dieses Verfahrens ist, klare Anweisungen für den Umgang mit jeglicher Hardware zu geben, auf der vertrauliche Daten gespeichert sind. Dazu gehören Regeln, die die sichere Vernichtung von Daten vor der Weitergabe oder der Entsorgung der Hardware gewährleisten sollen, um eine spätere Wiederherstellung der Daten zu verhindern.

10. Zugangskontrolle und Identitätsmanagement

10.1. Kennwortpolitik

Die Mitarbeitenden müssen unsere Politik für die Kennwortverwaltung umsetzen, um die Sicherheit unserer Konten und Daten während ihres gesamten Lebenszyklus zu gewährleisten.

Ebenso verpflichten wir uns, unsere Nutzer*innen über die spezifischen Anforderungen im Zusammenhang mit unserer Kennwortpolitik zu unterrichten und dabei ihre Kompetenzen, ihre Rolle und die Sensibilität der Ressourcen, auf die sie zugreifen können, zu berücksichtigen.

Nachfolgend einige Beispiele empfohlener bewährter Praktiken im Rahmen unserer Kennwortpolitik:

- zwingende Verwendung eines zulässigen Kennwortmanagers, um starke Kennwörter zu generieren und zu speichern;
- Erstellung sicherer Kennwörter, die aus mindestens zwölf alphanumerischen Zeichen und Sonderzeichen bestehen;
- keine Verwendung allgemein gebräuchlicher oder leicht zu erratender Begriffe;
- keine Weitergabe von Kennwörtern an andere Personen bzw. keine Verwendung von Kennwörtern für mehrere Konten;
- nach Möglichkeit Einrichtung einer Multi-Faktor-Authentifizierung.

Wir raten allen unseren Nutzer*innen dringend, diese Hinweise genau zu befolgen, um zur Aufrechterhaltung einer hohen Sicherheitsstufe unserer Organisation beizutragen.

10.2. Verwaltung von Rechten

Die Zuweisung von Zugriffen erfolgt nach Abteilungen, wobei nur die Berechtigungen erteilt werden, die für die einzelnen Aufgaben erforderlich sind.

Jegliche Bewilligungsgesuche sind über vorab festgelegte interne Kanäle einzureichen und nach eingehender Prüfung zu genehmigen.

10.3. Überprüfung der Rechte

Die Zugangsrechte werden einmal jährlich durch den RSSI und die Sicherheitsbeauftragten überprüft.

Es werden jährliche Sicherheitsprüfungen für die verschiedenen internen und externen Fachbereiche, Desktop-Computer sowie die Zugänge zu drahtlosen Netzwerken und WLAN durchgeführt.

Die erweiterte Verwaltung interner Zugänge ist Gegenstand einer automatischen jährlichen Überprüfung mit internen Tools.

10.4. Löschung von Zugriffen

Die Löschung der Zugriffe von Mitarbeitenden von Infomaniak Network ist an den HR-Prozess für die Verwaltung von Ein- und Austritten gebunden. Dieser Austrittsprozess wird mithilfe spezieller interner Tools unter der Leitung von Verantwortlichen, die die erforderlichen Massnahmen einleiten, streng überwacht.

11. Verschlüsselung

11.1. Verwendung von Verschlüsselung

Es werden Regeln für den effizienten Einsatz von Verschlüsselung, insbesondere die Verwaltung von kryptographischen Schlüsseln, festgelegt und angewandt.

Infomaniak Network hat eine Politik für die kryptografische Prüfung und Verschlüsselung festgelegt und umgesetzt, die allen Mitarbeitenden kommuniziert wurde und bekannt ist.

11.2. Verwendung verschlüsselter Protokolle

Infomaniak Network und seine Mitarbeitenden achten darauf, so oft wie möglich sichere Netzwerkprotokolle zu verwenden, und zwar sowohl in öffentlichen Netzwerken wie dem Internet als auch im internen Netzwerk. So bevorzugen wir die Nutzung von HTTPS für die Navigation im Web sowie von IMAPS, SMTPS oder POP3S für E-Mails und SSH (Secure Shell) für die Systemverwaltung.

11.3. Mobilität

Die Mitarbeitenden der Firma Infomaniak Network verwenden ausschliesslich ihre Notebooks, um sich aus der Ferne mit dem internen Sicherheitsnetzwerk des Unternehmens zu verbinden.

12. Physische und umgebungsbezogene Sicherheit

12.1. Standort

Die Datacenter von Infomaniak Network befinden sich ausschliesslich in der Schweiz und gehören vollständig dem Unternehmen.

12.2. Datacenter

12.2.1. Physische Sicherheit der Standorte und Zugangskontrolle

Räumlichkeiten werden laufend mit einem Videoüberwachungssystem überwacht, um unbefugtem physischen Zutritt vorzubeugen.

Der Zugang zu den Data Centern und Servern ist durch mehrere Schleusen und ein elektronisches Zutrittskontrollsystem mit biometrischer Identifikation geschützt. Um die Sicherheit des Datacenters weiter zu erhöhen, ist jeder Bereich und jeder Rack-Gang mit einem Gesichtserkennungssystem ausgerüstet.

Der Zugang zu den Serverräumen ist auf eine begrenzte Anzahl Mitarbeitende beschränkt, die für die nach den spezifischen Bedürfnissen der einzelnen Teams segmentierten Arbeitsbereiche speziell geschult und ermächtigt sind.

12.2.2. Gerätesicherheit

Datacenter sind alle nach ISO 27001 und ISO 14001 zertifiziert und verfügen über eine N+1 Redundanz der Stromversorgung, der Glasfaser-Backbone, der Kühlung, der Stromerzeugungsaggregate und der Wechselrichter, um einen unterbrechungsfreien Betrieb Ihrer technischen Infrastrukturen zu gewährleisten.

12.2.3. Automatisches Melde-, Alarm- und Löschsystem

Unsere Standorte werden überwacht und sind vollständig mit Brandmeldesystemen ausgestattet. Unsere auf die jeweilige Umgebung eines Datacenters abgestimmten Löschsysteme sorgen für das automatische Löschen von Bereichen, in denen ein Brand entstehen könnte. Diese Systeme kommen in Räumen zum Einsatz, in denen sich elektrische Anlagen wie Wechselrichter, Batterien oder elektrische Verteilertafeln befinden. Dieses Überwachungssystem ist ständig in Betrieb und wird regelmässig getestet.

12.3. Büroräume

12.3.1. Physische Sicherheit der Standorte und Zugangskontrolle

Die Büros am Hauptsitz von Infomaniak Network sind mit selbstverriegelnden Türen ausgestattet, die ausschliesslich über ein Badge- und Gesichtserkennungssystem zugänglich sind. Dabei werden regelmässig physische Zugangskontrollen durchgeführt.

In den Gängen sowie in den allgemeinen Bereichen des Gebäudes sind Überwachungskameras installiert, auch im Umfeld der Arbeitsbereiche der Mitarbeitenden.

12.4. Leerer Schreibtisch und leerer Bildschirm

Es besteht eine Politik der leeren Schreibtische und Bildschirme, die allen Mitarbeitenden kommuniziert wurde. Diese umfasst detaillierte Anweisungen zur Bildschirmsperre, zum richtigen Umgang mit papiergestützten und digitalen Dokumenten, zur Nutzung von Whiteboards und zur sicheren Vernichtung vertraulicher Dokumente.

13. Betriebssicherheit

13.1. Überwachung der Cybersicherheit

Informationen über Bedrohungen im Bereich der Informationssicherheit werden gesammelt, ausgewertet und verarbeitet, um Informationen über diese Bedrohungen zu erzeugen.

Wir nutzen einen Dienst von Drittanbietern, der uns die Möglichkeit bietet, Aktivitäten und Bedrohungen im Darkweb zu überwachen.

Die Suche nach solchen potenziellen Bedrohungen erfolgt anhand spezifischer Schlüsselwörter und Begriffe, insbesondere im Zusammenhang mit:

- der Gefährdung der Mitarbeitenden;
- der Überwachung der Marke und der Domainnamen;
- der Überwachung des Darknets;
- der Nutzung des Deep Web und der Auffindung der Vermögenswerte.

13.2. Daten

13.2.1. Datenklassifizierung

Informationen werden entsprechend den Informationssicherheitsbedürfnissen der Organisation auf Grundlage der Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit und wichtiger Anforderungen der beteiligten Parteien klassifiziert.

13.2.2. Verschlüsselung der Daten

Daten werden während der Übertragung zwischen den Arbeitsstationen von Mitarbeitenden, Kund*innen und dem Informationssystem von Infomaniak Network mithilfe der in Kapitel 11 dieses Dokuments beschriebenen Verschlüsselungsprotokolle gesichert.

13.2.3. Datenintegrität

Infomaniak Network verpflichtet sich, die Daten seiner Kund*innen zu schützen, indem sichere Verfahren, technische Massnahmen und Protokolle eingeführt werden, um jegliche

vorsätzlichen oder ungewollten Veränderungen zu verhindern. Dies schliesst solide Garantien in Bezug auf die Übermittlung und Speicherung vertraulicher Informationen ein.

13.3. Änderungsmanagement

Unsere Politik für Änderungsmanagement bietet Nutzer*innen eine Reihe gut dokumentierter operativer Abläufe und strenge Kontrollen. Sie umfasst:

- Rahmenbedingungen für Änderungen, in denen ihre Tragweite und Ziele klar festgelegt sind;
- Richtlinien für die Umsetzung von Änderungen, einschliesslich Akzeptanzkriterien und Sicherheitsregeln;
- die detaillierte Planung der Änderungen, einschliesslich der Ermittlung potenzieller Risiken und geeigneter Notfallpläne;
- die strenge Kontrolle von Änderungen mit vollständiger Nachvollziehbarkeit aller Änderungen am System;
- klare und einfach nachvollziehbare Prozesse für regelmässige Aktualisierungen des Systems, die dessen optimale Stabilität und Leistung gewährleisten.

13.4. Schutz vor bösartiger Software

Es wird ein Schutz vor Schadprogrammen eingerichtet und durch entsprechende Sensibilisierung der Nutzer*innen verstärkt. Der IT-Bestand an Arbeitsstationen wird von einem zentralen Virenschutzprogramm überwacht, wobei bei den Sicherheitsmeetings regelmässige Kontrollen und Indikatoren festgelegt und überprüft werden.

13.5. Backup-Politik

Es ist eine Politik für Datensicherung und -sicherheit in Kraft, die mit klaren Richtlinien für die Sicherung und Wiederherstellung von Informationen im Einklang mit den in unserem Informationssystem identifizierten Vermögenswerten einhergeht. Mit dieser Politik werden die Aufbewahrungsdauer, die Häufigkeit, die Art der Verschlüsselung sowie die zu befolgenden Testprotokolle festgelegt.

Mit diesen Massnahmen können wir den wirksamen Schutz und die wirksame Wiederherstellung unserer wichtigen Daten gewährleisten.

13.6. Protokollierung

Es werden Logs generiert, gespeichert, geschützt und ausgewertet, die Aktivitäten, Ausnahmen, Störungen und andere relevante Ereignisse aufzeichnen.

13.7. Uhrensynchronisation

Die Zeitschaltuhren der von der Organisation verwendeten IT-Systeme werden mit zulässigen Zeitquellen synchronisiert.

Infomaniak Network verfügt über eigene Zeitreferenzserver, die eine präzise Zeitsynchronisation für alle Geräte und Server ermöglichen. Dieser Dienst ist auch öffentlich zugänglich und steht sowohl Kund*innen als auch Nichtkund*innen zur Verfügung.

13.8. Beaufsichtigung

13.8.1. Grundsätzliches

Sämtliche von Infomaniak Network verwalteten Dienste und Systeme unterliegen der sorgfältigen Überwachung. Unsere Überwachungstools basieren auf Standardprotokollen und eigens entwickelten Steuerungen, um Daten aus allen Prüfquellen zu erfassen.

Bei Störungen werden für alle überwachten Dienste Echtzeitalarme ausgelöst.

Diese Alarme können auch ausserhalb der Arbeitszeit als SMS an die Bereitschaftsdienstteams gesendet werden.

13.8.2. Bereitschaftsdienste

Das Bereitschaftsdienstteam gewährleistet in Bezug auf das Informationssystem (SI) von Infomaniak Network eine kontinuierliche Überwachung und Interventionen an sieben Wochentagen rund um die Uhr. Das Team ist in verschiedene Stufen unterteilt und umfasst Fachleute aus unterschiedlichen Produktionsteams, sodass sämtliche Kompetenzbereiche abgedeckt sind.

14. Kommunikationssicherheit

14.1. Technische Architektur

Die Infrastruktur für den Betrieb der Dienste von Infomaniak Network ist aufgesplittet und in mehrere separaten Sicherheitszonen unterteilt. Diese Auslegung bietet erhöhte Sicherheit, ist skalierbar und an aktuelle und künftige Anforderungen angepasst. Gruppen von Informationsdiensten, Nutzer*innen und Informationssystemen werden in organisationsinternen Netzwerken isoliert, wodurch ein hohes Mass an Schutz vor möglichen externen oder internen Bedrohungen gewährleistet ist.

14.2. Internet

Infomaniak Network verfügt über eigene öffentliche IP-Adressen sowie über mehrere Internetverbindungen verschiedener Anbieter. So kann das Unternehmen seinen Kund*innen und Mitarbeitenden auch bei Ausfall eines Anbieters ein optimales Serviceniveau gewährleisten. Zudem sind alle von Infomaniak verwalteten Leistungen redundant ausgelegt, was ihre Kontinuität sichert.

14.3. WLAN-Netzwerke

Die WLAN-Netzwerke von Infomaniak werden entsprechend ihren spezifischen Verwendungen wie Gast-WLAN, Mitarbeiter-WLAN, Vorproduktions-WLAN usw. segmentiert, wobei die Zugriffskontrolle auf Grundlage der Rechteverwaltung erfolgt. Darüber hinaus sind WLAN-Zugangspunkte vor unbefugtem Zugriff geschützt.

14.4. Sicherheitseinrichtungen

14.4.1. Firewall

Bei Infomaniak sind zwischen jeder Sicherheits- und jeder Anwendungszone Firewalls installiert. So müssen von aussen eingehende Datenströme mehrere Firewall-Ebenen durchlaufen, bevor sie den gewünschten Fachbereich erreichen, sodass ein besserer Schutz vor potenziellen Bedrohungen gewährleistet ist.

14.4.2. IDS

An Schlüsselstellen des Infomaniak-Netzwerks befinden sich IDS-Sensoren, um die ein- und ausgehenden Datenströme des Informationssystems zu analysieren. Diese Sensoren haben die Aufgabe, verdächtige oder anormale Aktivitäten sowie böswilligen Datenverkehr zu erkennen und umgehend die Produktionsteams zu benachrichtigen. Dazu erhalten die Sensoren regelmässig Updates der Angriffssignaturen von unserem auf Cybersicherheit spezialisierten Dienstleister. Die Installation und Wartung dieser Systeme unterliegt der Verantwortung des Produktionssicherheitsteams.

14.4.3. DDoS-Schutz

Infomaniak richtet für alle von ihm betriebenen Technologien einen angemessenen DDoS-Schutz ein und gewährleistet so den Schutz aller seiner Plattformen und Infrastrukturen vor derartigen Cyberbedrohungen. Auf diese Weise will Infomaniak eine hohe Verfügbarkeit und Resilienz ihrer Dienste zum Nutzen von Kund*innen und Mitarbeitenden aufrechterhalten.

15. Beschaffung, Entwicklung und Wartung von Informationssystemen

15.1. Sicherer Entwicklungslebenszyklus

Es werden Regeln in Bezug auf Sicherheit, bewährte Verfahren und gesunden Menschenverstand festgelegt und angewandt, um die sichere Entwicklung von Software und Systemen zu gewährleisten. Diese Grundsätze umfassen unter anderem:

- die Prüfung und Registrierung von Massnahmen
- die Schulung von Entwickler*innen in Bezug auf Sicherheit

- die Bekämpfung von Schadprogrammen
- Prüfungen der Sicherheit von Anwendungen
- Prüfungen der Konformität des Systems
- die Sicherheit client- und serverseitiger Webanwendungen
- die Sicherheit mobiler Anwendungen
- Verschlüsselung

Die Mitarbeitenden der Entwicklungsabteilung werden über die Risiken im Zusammenhang mit der Sicherheit von Anwendungen und die Standards des OWASP (Open Web Application Security Project) aufgeklärt.

Darüber hinaus haben wir eine Politik für die Überwachung und Kontrolle der externen Entwicklung eingeführt, der zufolge Ausführungsmodalitäten, bestehende Sicherheitsmassnahmen sowie verbindliche Anweisungen für die Verwaltung der Protokolle, Zugriffe und Quellcodes und die Sicherheitstests während des Entwicklungszyklus empfohlen werden.

15.2. Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Unsere Netze und Entwicklungsinfrastrukturen sind je nach den erbrachten Diensten sowohl physisch als auch logisch isoliert. Zudem trennen wir die verschiedenen Anwendungsumgebungen wie für Entwicklung, Tests, Vorproduktion und Produktion separat.

Konkret ist die Entwicklungsumgebung streng eingegrenzt und nur für Entwickler*innen über unser hochsicheres internes Netzwerk zugänglich.

16. Beziehung zu Anbietern

Wir haben Prozesse und Verfahren eingeführt, um potenzielle Risiken für Informationssicherheit zu steuern, die sich aus der Nutzung unserer Produkte oder Dienstleistungen bei bestimmten Anbietern ergeben.

Darüber hinaus achten wir streng darauf, mit allen unseren Anbietern angemessene Anforderungen an Informationssicherheit einzurichten und zu vereinbaren.

Ebenso führen wir eine regelmässige Überprüfung und Bewertung sowie ein proaktives Management von Änderungen an den Informationssicherheitspraktiken unserer jeweiligen Anbieter und Dienstleister durch.

17. Schwachstellen- und Vorfallmanagement

17.1. Schwachstellenmanagement

Seitens der Produktionsteams wurde ein Workflow für das Management von CVE-Schwachstellen mithilfe interner Tools und Technologieüberwachung eingeführt.

Verschiedene interne Tools ermöglichen, Schwachstellen, die unsere Informationssysteme betreffen können, nachzuverfolgen, zu überwachen und automatisch zu bereinigen.

Für die Verarbeitung der Meldung von Schwachstellen wurde ein interner SLA (Service Level Agreement) mit einer Reaktionszeit in Abhängigkeit von der Schwere der identifizierten Schwachstellen eingeführt.

17.2. Schwachstellenscanner

Es werden regelmässig Analysen über mehrere von uns spezifizierte IP-Adressbereiche von Infomaniak durchgeführt. Wir werden über ein Dashboard benachrichtigt, wenn Schwachstellen erkannt werden, und setzen Aktionspläne ein, um aufgedeckte Schwachstellen rasch zu beheben.

17.3. Bug-Bounty-Programm

Wir arbeiten aktiv mit einer Community aus Forscher*innen und ethischen Hacker*innen zusammen, um unseren Kund*innen ein optimales Sicherheitsniveau zu bieten. Es stehen sowohl ein öffentliches Programm als auch private Programme zur Verfügung, um alle unseren Kund*innen angebotenen Dienste zu testen.

Hinweisgeber*innen sind angemessen geschützt, und unsere Mitarbeitenden haben jederzeit die Möglichkeit, mutmassliche Unregelmässigkeiten vertraulich und anonym zu melden.

17.4. Umgang mit Sicherheitsvorfällen

Die Rollen, Verantwortlichkeiten, der Triage-Prozess, die Kommunikation, die Reaktion und die Entschärfung sowie der gesamte Workflow, der für die vollständige Lösung des Vorfalls erforderlich ist, sind in einem bewährten Verfahren für den Umgang mit Sicherheitsvorfällen zweifelsfrei festgelegt.

Je nach Schwere und Art des Ereignisses kann Infomaniak Network aktiv mit den zuständigen Behörden zusammenarbeiten und den Prozess für die Behandlung des Vorfalls koordinieren, um dessen rasche und effiziente Lösung zu gewährleisten.

17.5. Krisenmanagement

Es ist ein spezifisches Verfahren für Krisenmanagement festgeschrieben. Dieses Verfahren umfasst die einzelnen Schritte, die befolgt werden müssen, um den Vorfall möglichst effizient zu lösen und die Ursache und Auswirkungen bestmöglich intern und extern zu kommunizieren.

18. Management der Geschäftsfortführung

18.1. Kontinuität der Steuerung

Für das Management und die Steuerung der Dienste und Vermögenswerte der Infrastruktur unserer Datacenter wird ein Kontinuitätsplan festgelegt.

18.2. Plan zur Aufrechterhaltung des Geschäftsbetriebs (PCA) und Resilienz

Die Aufrechterhaltung des Geschäftsbetriebs wird bereits in der Konzeptions- und Architekturphase der von Infomaniak Network verwalteten Dienste berücksichtigt.

Die Redundanz zwischen unseren verschiedenen Datacentern sowie die Sicherung auf mehreren Datenträgern und in mehreren Datacentern tragen dazu bei, die Aufrechterhaltung des Geschäftsbetriebs für unsere Kund*innen zu gewährleisten.

Die Lösungen für die Wiederaufnahme nach Schadenfällen unserer verwalteten Dienste hängen von den technischen und softwarespezifischen Architekturen ab und werden an die jeweilige Stufe des Angebots entsprechend den spezifischen Anforderungen und den Produktionsteams angepasst.

18.3. Folgenabschätzung für die Tätigkeit

Um Daten zur effizienten Planung und Bewältigung von Sicherheitsvorfällen zu erfassen, die sich auf die Vermögenswerte unseres Informationssystems auswirken, wurde eine Folgenabschätzung für die Tätigkeit (BIA) erstellt.

Diese Folgenabschätzung ermöglicht die Identifizierung wichtiger Aktivitäten und Ressourcen des Unternehmens sowie der verschiedenen damit verbundenen Schweregrade. Darüber hinaus wurden spezifische Massnahmen festgelegt, um die Aufrechterhaltung des Geschäftsbetriebs bei Vorfällen zu gewährleisten.

18.4. RPO und RTO

Infomaniak Network hat eine Kontinuitätsstrategie entwickelt und dabei drei wichtige Faktoren berücksichtigt:

- die maximal zulässige Ausfallzeit (TMA), auch als der für die Wiederherstellung vorgegebene Zeitraum (RTO) oder in Englisch als Recovery Time Objective (RTO) bezeichnet;
- den maximal akzeptablen Datenverlust (PMAD), auch als Vorgabe für den Wiederherstellungspunkt (OPR) oder in Englisch als Recovery Point Objective (RPO) bezeichnet;
- potenzielle finanzielle und geschäftliche Auswirkungen.

Soweit relevant, werden diese Elemente in der Folgenabschätzung für die Tätigkeit (BIA) erfasst.

18.5. Testplan

Jedes Jahr wird unter Berücksichtigung von Risikosituationen ein Testplan erstellt und umgesetzt. Er ermöglicht Folgendes:

- vorab die Messung der Wirksamkeit des Plans im Hinblick auf die Kontinuitätsziele anhand von Indikatoren, Audits usw.
- in Krisen die Überwachung der tatsächlich erreichten Dienstgüte und der Funktionsweise der im Rahmen des PCA vorgesehenen Betriebsabläufe.
- im Nachhinein die Einsetzung eines Verbesserungsplans.

19. Compliance

19.1. Normen und Regelwerke

19.1.1. ISO 27001

Die Teams von Infomaniak Network orientieren sich bei der Entwicklung und Verwaltung der Dienste, die sie ihren Kund*innen anbieten, an international anerkannten Sicherheitsnormen wie ISO 27001:2022 und ISO 27002:2022.

Diese Normen bilden einen soliden Rahmen für die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten sowie für ein wirksames Management der Risiken für die Informationssicherheit.

19.1.2. DSG und DSGVO

Infomaniak Network hat eine Datenschutzrichtlinie verabschiedet, die auf seiner Website unter folgender Adresse einsehbar ist:
https://www.infomaniak.com/de/agb/datenschutzrichtlinien

Darüber hinaus ist die Cookie-Richtlinie unter folgendem Link abrufbar:
https://www.infomaniak.com/de/agb/politik-nutzung-cookies

19.2. Audit

19.2.1. Internes Audit

Die Kontrolle der Sicherheitsaktivitäten innerhalb der Zertifizierungsbereiche von Infomaniak Network erfolgt durch qualifizierte Consultants, die unter Aufsicht des Compliance-Teams tätig sind.

Diese Consultants überprüfen regelmässig die Elemente, die mit den zertifizierten Bereichen verbunden sind, und zwar gemäss dem Auditplan und der Erklärung zur Anwendbarkeit von Infomaniak Network.

Dokumente in Bezug auf interne Audits sind vertraulich und dürfen nicht weitergegeben werden.

19.2.2. Externes Audit

Im Rahmen der Zertifizierung nach ISO 27001:202 wird Infomaniak Network jährlich von Zertifizierungsstellen geprüft.

19.2.3. Technisches Audit

Infomaniak Network beauftragt qualifizierte Expert*innen mit der Durchführung regelmässiger technischer Audits seines Informationssystems sowie bei Bedarf und bei der Einrichtung neuer Dienste.

19.2.4. Kundenaudit

Kund*innen haben die Möglichkeit, Penetrationstests (Pentests) für die von ihnen genutzten Dienste durchzuführen, wobei die vertraglich festgelegten Bedingungen strikt einzuhalten sind.

Ebenso müssen sie die Sachzwänge der internen Teams berücksichtigen, wie die ausschliessliche Durchführung von Pentests während der Bürozeiten und die vorherige Unterrichtung der Produktionsteams.