Appendix - Technical and Organizational Measures (TOMs)

Summary

1. History 3
2. Introduction of this document 4
3. Confidentiality 5
3.1. Physical Security 5
3.2. System access control 5
3.3. Security testing 5
3.4. Encryption 5
4. Integrity 6
4.1. Change and version management 6
4.2. Recording and monitoring 6
4.3. Transfer control 6
4.4. Data protection management 6
5. Availability and reliability 7
5.1. Incident response management 7
5.2. Risk management 7
5.3. Business continuity 7
5.4. Threat and weakness management 7
5.5. Audit 7

1. History

Date	Author	Responsibility	Type of change
05.01.2024	Johann Laqua	RSSI	First version of the document

2. Introduction of this document

This document complies with the requirements set forth in Article 32 of the GDPR, as well as Articles 7 and 8 of the Swiss Federal Data Protection Act (LPD).

It describes the technical and organizational measures that apply to all services and customers of Infomaniak.

3. Confidentiality

3.1.Physical Security

- Control of physical access is implemented in the company's premises through systems such as using badges or facial recognition.
- Access to data centers is strictly limited.
- Surveillance is provided by video cameras and an alarm goes off in case of break-in.
- Access is personalized, documented, and segregated according to the respective roles of employees.
- Visitors are only allowed to remain in the premises if accompanied by an employee.

3.2.System access control

- A policy for controlling both physical and logical access is established and disseminated throughout the organization.
- A password control policy is applied.
- The use of two-factor authentication methods is mandatory for all connections to various services.
- Automatic locking of workstations occurs after several minutes of inactivity.
- Policies related to clean desk and clear screen have been put in place.
- A policy governing mobile working and remote work has also been established.
- The computer park benefits from anti-virus software protection.

3.3.Security testing

- Utilization of a public bug bounty program.
- Internal security testing within project workflows.
- External security testing through partnerships with cybersecurity firms.

3.4.Encryption

- All workstations are encrypted.
- Remote connections to the company's network are encrypted via VPN.
- Policy for cryptographic control and encryption

4. Integrity

4.1. Change and version management

- Change management policy applied and integrated into services.

4.2. Recording and monitoring

- Recording of data access and modifications.
- Centralised audit and security logs.
- Checks on the completeness and accuracy of data transfer (end-to-end control).

4.3. Transfer control

- Classification of information by security level.
- A confidentiality level is assigned to each item of information according to its nature.
- Mandatory use of encrypted internal tools for data transfer.

4.4. Data protection management

- Data protection officers and an information systems security officer are appointed.
- An organisation dedicated to data protection and information security has been set up.
- All employees are made aware of the information security culture.
- Employees are made aware of the processing of personal data.
- A register of processing activities is kept up to date, and data protection assessments are carried out where necessary.
- Procedures for exercising the rights of data subjects have been put in place.

5. Availability and reliability

- Use of hardware and software firewalls.
- Intrusion detection systems.
- Emergency manuals for data recovery, protection against accidental destruction and loss.

5.1. Incident response management

- Procedure for responding to a security incident.
- Crisis management procedure.
- All data centres are ISO 27001 certified.
- Temperature monitoring of assets in data centres.

5.2. Risk management

- Establishment of a risk assessment and evaluation to identify, evaluate, and categorize potential risks to privacy, integrity, and availability of information within the organization.
- Implementation of an action plan and control measures adapted to identified risks.

5.3. Business continuity

- Uninterruptible power supply (UPS) and backup generators to maintain service availability in case of power failures.
- Redundancy built into critical systems to minimize single points of failure.
- Distributed Denial of Service (DDoS) attack mitigation solutions to maintain the availability of managed services.
- Regular testing of data backups.
- Periodic recovery exercises.
- Business Continuity Plan (BCP) defined, managed, and monitored by production teams.

5.4. Threat and weakness management

- Regular scans of our infrastructure to detect vulnerabilities.
- System updates with the various production teams.
- Cooperation with partners to detect external threats.
- Technological monitoring of our assets and internal tools.

5.5. Audit

- Performing internal audits by qualified consultants covering ISO 27001 certified scope areas.
- Annual external audits conducted by ISO 27001 certifying bodies.

- Ad hoc technical audits executed by qualified experts on information systems, as needed.