Security Insurance Plan

Infomaniak Network

Table of contents

1. History

Date	Author	Function	Nature of the change
13/05/2025	Johann Laqua	CISO	Company logo change, physical security chapters updated, definitions chapter added
19/04/2024	Johann Laqua	CISO	Document finalised for first publication
14/02/2024	Johann Laqua	CISO	First draft of the document

2. About this document

The purpose of this document is to present Infomaniak Network SA’s Security Insurance Plan.

3. Intro

3.1. Purpose of the document

This document establishes our Safety Insurance Plan (SIP), which can be attached to our contracts with our customers. This plan defines the commitments made by Infomaniak Network to meet contractual requirements in terms of information systems security (ISS). These are intended to:

- ensure the protection of information systems assets used in the provision of contractually agreed services;
- protect our customers from any harm that may result from the unavailability of these resources, as well as from any violation of their integrity or confidentiality.

Our Security Insurance Plan (SIP) details the various security-related provisions, including the physical, organisational, procedural and technical measures we have put in place.

3.2. Scope of application

This document concerns the services managed by the Infomaniak Network teams as well as their activities.

3.3. Evolution

Changes to the Safety Insurance Plan (SIP) result in a new version of this document. Any changes made are recorded and dated in the version history included with the document.

The Security Insurance Plan (SIP) is reviewed at least once a year by those responsible for compliance and information systems security and then approved by the management team.

3.4. Definitions

CISO: Chief Information Security Officer
ISO : International Organization for Standardization
ENISO: Expression of Needs and Identification of Security Objectives
Red team: security team focused on offensive security drills and tests involving people from different departments.
ASDPO: Swiss Association of Data Protection Officers
NCSC: National Cyber Security Centre
CERT: Computer Emergency Response Team
HR: Human Resources
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
FADP: Federal Act on Data Protection
GDPR : General Data Protection Regulation

4. Best practices

Infomaniak Network's security is managed for the entire company by a security committee and a compliance team in accordance with the standards of the ISO 27001 standard. Infomaniak Network is certified ISO 27001:2022 in the following areas and activities:

development and provision of cloud infrastructure, web services, applications, customer support, data center operational maintenance.

5. Risk management

Infomaniak Network has formalised a written risk assessment that covers the entire scope of application of the security insurance plan, applying a documented methodology guaranteeing the reproducibility and comparability of the approach.

The risk assessment process involves risk analysis, management and mitigation plans leading to tangible measures and projects.

Furthermore, Infomaniak Network relies on widely recognised methods, such as EBIOS RM, to manage risks as part of its information security management system (ISMS).

6. Information security policy

Infomaniak Network has a security policy, which can be found at the following address: https://www.infomaniak.com/documents/politique_SI_EE_en.pdf

This document clearly sets out our information security commitments and objectives.

7. Information security organisation

To structure our approach to information systems security (ISS), we have put in place several complementary tools: an ISS-specific organisation chart, an internal information systems security policy (ISSP), and an information security management system (ISMS).

These elements are essential to ensure the thorough and consistent application of our security procedures.

7.1.Roles and responsibilities

Security responsibilities have been defined and assigned.

Infomaniak Network has appointed a Chief Information Security Officer (CISO). This individual oversees all technical and organizational measures implemented as part of our comprehensive information security strategy.

A security committee, composed of the heads of various departments and technical teams within the company, meets weekly for SOC (Security Operations Center) meetings to discuss topics related to information security.

Under the supervision of the CISO, a Red Team conducts security tests on products and social engineering tests on the company's employees.

7.2.Governance

A dedicated governance team has been established at strategic and operational levels.

This team meets regularly to oversee information systems security issues. The minutes of these meetings are stored securely.

7.3.Relationship with agencies and authorities

Infomaniak Network is a member of professional associations (ASDPO) and maintains relationships with the authorities (NCSC and Cyber Security Hub) for developments in the field of information security.

7.4.Monitoring and security

Technical and legal security monitoring is in place and conducted within the business. This helps prevent risks linked specifically to Infomaniak Network’s activities.

Infomaniak Network relies on a partnership with a cybersecurity specialist to monitor the Dark Web for sensitive assets under its responsibility.

8. Human resources security

8.1.Recruitment

Our HR department applies a recruitment process for every candidate, with security measures proportionate to each employee's classification level and the risks identified.

The following checks are conducted:

- candidate identity check
- job competency check
- candidate's reference check
- criminal record check
- extensive background checks for candidates at high security levels

8.2.Confidentiality management

Employment contracts clearly stipulate the information security responsibilities of staff.

A confidentiality clause, taken from the general terms and conditions of the employment contract, obliges staff to strictly respect the confidentiality of the sensitive and private data to which they have access in the course of their duties at Infomaniak. Any violation of this clause will have consequences for the offender.

Furthermore, a formal disciplinary process has been established and communicated to all staff and other relevant stakeholders. This process includes appropriate sanctions for anyone who violates the information security policy.

8.3.Safety awareness

We conduct security induction sessions to verify the compliance of workstations, while sensitising colleagues to the risks concerning information systems security (ISS) as well as our physical and logical security procedures.

During these sessions, we also present important documents such as our Information Security Policy (ISP) and our General Security Guidelines.

Each year, we develop an awareness programme using a variety of assessment tools on a range of security and cyber security topics. These include phishing and social engineering campaigns, among others.

Several communications are sent to employees by email with the aim of making them aware of information security risks, data protection, cyber risks and updates to our information security management system.

8.4.IT charter

Infomaniak Network has General Security Guidelines, equivalent to an IT charter, which are regularly updated and communicated to all members of our company.

As soon as they are hired and every year, they solemnly undertake to respect these guidelines, failing which they may be subject to disciplinary sanctions.

8.5.Skills and training

Every year, during personal interviews, the HR department conducts a survey of employees to assess their training needs. An annual training programme is then established to identify the training required to address:

- gaps in the competencies of an employee, team or department;
- continuous skills development needs.

The training offered may be provided in-house or by external providers.

Several technical training courses are offered throughout the year by delegates or cybersecurity experts, along with quarterly reports and statistics on vulnerabilities that could impact our systems, in order to strengthen the skills of our staff.

8.6.End of contract

An exit or termination procedure has been adopted and communicated to all relevant managers within the company. The purpose of this procedure is to ensure that the employee no longer has physical or software access to the company's information system.

9. Asset management

9.1.Inventory

Infomaniak Network draws up inventories of essential assets and support goods. These are recorded in our Information Security Management System (ISMS) as well as in our risk assessments.

We review these assets annually through ISMS and update them by means of automated processes according to the requirements of the different internal teams.

9.2.Software licences

Infomaniak Network is determined to guarantee the use of valid licences for third-party software within its internal teams and takes the necessary measures to protect intellectual property rights.

9.3.Identification and classification of assets

Assets are segmented and clearly identified through a nomenclature and naming convention established by the in-house teams. Ongoing and annual controls are in place to ensure legitimacy of access, restriction of unauthorised access and reliability of the inventory.

Data is classified according to the organisation’s information security needs, taking into account confidentiality, integrity and availability requirements, as well as key stakeholder concerns.

9.4.Media updates, antivirus and encryption

The Information Systems Security Officer (ISSO) oversees the centralised protection of company assets, including employee workstations, against viruses and malware. A defence strategy against these threats is reinforced by appropriate training of users.

The security of internal and removable storage media is ensured by a configured and monitored encryption process.

Key performance indicators (KPIs) are tracked regularly to verify compliance and asset protection.

9.5.Teleworking

To ensure the security of information while teleworking, various precautions have been taken. Specific teleworking guidelines have been developed and communicated to staff. It is mandatory to use a secure virtual private network (VPN) to connect to organisational resources from the outside.

Furthermore, the use of personal devices (“Bring Your Own Device,” or BYOD) is not permitted in this context.

9.6.Management of removable media and equipment

Guidelines for the use of removable media have been put in place, disseminated and are well known to staff. These instructions include strict rules for their use to minimise potential risks and recommendations for their protection.

For example, it may be stipulated that removable media containing confidential or critical data must be encrypted or that their use be restricted to specific circumstances.

9.7.Disposal

An equipment recycling and asset decommissioning policy has been established and implemented to manage the company’s sensitive assets.

The purpose of this procedure is to provide clear instructions on how to handle all types of equipment that stores confidential data. This includes rules to ensure the secure destruction of data prior to the transfer or disposal of the equipment in order to prevent subsequent retrieval of the data.

10. Access control and identity management

10.1. Password policy

Employees must follow our password management policy to ensure the security of our accounts and data throughout their life cycle.

We are also committed to informing our users of the specific requirements of our password policy, taking into account their skills, role and the sensitivity of the resources they may access.

Here are some examples of best practices recommended as part of our password policy:

- Obligation to use an authorised password manager to generate and store strong passwords;
- create strong passwords consisting of at least 12 alphanumeric and special characters;
- avoid using commonly used or easily guessable terms;
- never share your password with anyone else or reuse it for multiple accounts;
- configure multi-factor authentication whenever possible;

we strongly encourage all our users to adhere strictly to these guidelines to help maintain a high level of security within our organisation.

10.2. Rights management

This allocation of access is organised by department, granting only the necessary permissions based on the tasks assigned to each individual.

Any authorisation request must be submitted through predefined internal channels and approved after thorough review.

10.3. Rights review

An annual review of access rights is conducted by the ISSO and security delegates.

Annual security checks are performed for various internal and external services, desktops, wireless network access and Wi-Fi.

The advanced management of internal accesses is subject to automatic and annual verification using in-house tools.

10.4. Removal of access

Removing access for Infomaniak Network employees is associated with the HR entry and exit management process. This exit process is rigorously monitored using dedicated in-house tools, under the management of officers designated to take the required actions.

11. Cryptography

11.1. Use of cryptography

Rules for the effective use of cryptography, including cryptographic key management, are defined and implemented.

Infomaniak Network has drawn up and implemented a Cryptographic Control and Encryption Policy, which has been published and is known to all its staff.

11.2. Use of encrypted protocols

Infomaniak Network and its employees make sure that they use secure network protocols as often as possible, both on public networks such as the Internet and within the internal network. For example, we support the use of HTTPS for web browsing, IMAPS, SMTPS or POP3S for messaging, and SSH (Secure Shell) for system administration operations.

11.3. Mobility

Infomaniak Network employees only use their laptops to connect remotely to the company’s internal security network.

12. Physical and environmental security

12.1. Location

The Infomaniak Network data centers are located exclusively in Switzerland and belong entirely to the company.

12.2. Data centers

12.2.1. Physical security of sites and access control

The premises are constantly monitored by a system of video surveillance cameras to prevent unauthorised physical access.

Access to the data centers and servers is protected by several airlocks and an electronic access control system with biometric identification. To further enhance data center security, each sector and aisle serving the racks is equipped with a facial recognition system.

Access to server rooms is restricted to a limited number of company staff, specially trained and authorised in the segmented work areas according to the specific needs of the different teams.

12.2.2. Equipment security

The data centers are all certified ISO 27001 and ISO 14001 and benefit from n+1 redundancy in terms of power supply, fibre optic backbone, cooling, generators and inverters in order to guarantee uninterrupted operation of your technical infrastructure.

12.2.3. Automatic detection, alarm and extinguishing system

Our sites are monitored and fully equipped with fire detection systems. Our extinguishing systems, calibrated for each data center environment type, ensure automatic extinguishing in areas where a fire could start. These systems operate in rooms containing electrical equipment such as inverters, batteries or distribution panels. This monitoring system runs continuously and is tested on a regular basis.

12.3. Offices

12.3.1. Physical security of sites and access control

The offices at the Infomaniak Network head office are equipped with automatically locking doors, which can only be accessed via a badge and facial recognition system: physical access checks are carried out on a regular basis.

Surveillance cameras are installed in the corridors as well as in the common areas of the building, including in the vicinity of employee workspaces.

12.4. Clear desk and blank screen

A clear desk and blank screen policy is in place and has been communicated to all staff. This includes detailed instructions on locking screens, proper management of paper and digital records, the use of whiteboards, and the secure destruction of confidential documents.

13. Security relating to operations

13.1. Cyber security intelligence

Information about information security threats is collected, analysed and processed in order to generate information about such threats.

We benefit from a third-party service that allows us to monitor activities and threats on the Dark Web.

These potential threats are searched for using pre-determined specific keywords and terms, including those relating to:

- employee exposure;
- trademark and domain name monitoring;
- Dark Net monitoring;
- exploring the deep web and discovering assets.

13.2. Data

13.2.1. Data classification

Information is classified in accordance with the organisation’s information security needs, based on the requirements of confidentiality, integrity, availability and important requirements of the interested parties.

13.2.2. Data encryption

Data is secured while being transferred between the workstations of employees, customers and the Infomaniak Network information system thanks to the use of encryption protocols described in section 11 of this document.

13.2.3. Data integrity

Infomaniak Network undertakes to protect its customers’ data by implementing secure procedures, technical measures and protocols to prevent any alteration, whether intentional or accidental. This includes strong safeguards for the transmission and retention of confidential information.

13.3. Change management

Our change management policy provides users with a well-documented set of operating procedures and rigorous controls relating to these. It includes:

- the framing of changes, which clearly defines their scope and objectives;
- guidelines for implementing changes, including acceptance criteria and security rules;
- detailed planning for changes, including identification of potential risks and appropriate contingency plans;
- strict change control, with full traceability of all changes made to the system;
- clear and easy-to-follow processes for regular system updates, ensuring optimum stability and performance.

13.4. Protection against malware

Anti-malware protection is implemented and enhanced by appropriate awareness-raising among users. The computer equipment at the workstations is monitored by a centralised antivirus system and regular checks; indicators are set up and reviewed during security meetings.

13.5. Backup policy

A Data Backup and Security Policy is in place, defining clear guidelines for backing up and restoring information in accordance with the assets identified in our information system. This policy specifies the retention period, frequency, type of encryption and test protocols to be followed.

Through these measures, we can ensure the effective protection and recovery of our important data.

13.6. Logging

Logs that record activities, exceptions, outages and other relevant events are generated, retained, protected and analysed.

13.7. Clock synchronisation

Clocks in the information processing systems used by the organisation are synchronised with approved time sources.

Infomaniak Network has its own time reference servers, which allow all devices and servers to benefit from precise time synchronisation. This service is also publicly accessible and available to customers and non-customers alike.

13.8. Monitoring

13.8.1. Principles

All the services and systems managed by Infomaniak Network are closely monitored. Our monitoring tools are based on standard protocols as well as automatons specially designed to collect data from all control sources.

In the event of a failure, real-time alerts are issued for all services monitored.

These alerts may also be sent by SMS to on-call teams during off-duty hours.

13.8.2. On-call teams

The on-call team ensures continuous monitoring and intervention 24/7 on the Infomaniak Network information system (IS). These teams are structured on different levels and bring together specialists from different production teams, covering all areas of expertise.

14. Communications security

14.1. Technical architecture

The infrastructure supporting Infomaniak Network's services is compartmentalised and organised into several separate security zones. This design provides enhanced security that is scalable and adapted to current and future requirements. Groups of information services, users and information systems are isolated within the organisation's internal networks, ensuring a high level of protection against potential external or internal threats.

14.2. Internet

Infomaniak Network has its own public IP addresses as well as several Internet connections from different providers. This allows the company to guarantee its customers and employees an optimal level of service, even in the event of a provider failure. What's more, all the services managed by Infomaniak benefit from redundancy, ensuring their continuity.

14.3. Wi-Fi networks

Wi-Fi networks at Infomaniak are segmented according to their specific uses, such as Wi-Fi networks for guests, employees, pre-production, etc., with access control based on rights management. In addition, Wi-Fi hotspots are secured to prevent unauthorised access.

14.4. Safety equipment

14.4.1. Firewall

At Infomaniak, firewalls are installed between each security zone and each application zone. For example, incoming flows from outside must pass through several firewall levels before reaching the requested department, which provides enhanced protection against potential threats.

14.4.2. IDS

IDS probes have been deployed at key locations in the Infomaniak network in order to analyse the incoming and outgoing flows of the information system. These probes are responsible for detecting suspicious or abnormal activity, as well as malicious traffic, and immediately informing the production teams. To this end, the probes receive regular updates of attack signatures from our specialist cybersecurity provider. The Production Safety Team is responsible for installing and maintaining these devices.

14.4.3. Anti-DDoS

Infomaniak implements appropriate anti-DDoS protection for each of the technologies it uses, thus ensuring that all its platforms and infrastructures are protected against this type of cyber threat. In doing so, it aims to maintain a high level of availability and resilience for its services, for the benefit of both its customers and staff.

15. Acquisition, development and maintenance of information systems

15.1. Secure development life cycle

Security rules, best practices and common sense are established and implemented to ensure the safe development of software and systems. These principles include:

- auditing and recording actions;
- security training for developers;
- the fight against malware;
- application security testing;
- system compliance testing
- customer and server-side web application security;
- mobile app security;
- cryptography.

Development department staff are made aware of application security risks and the standards set by the Open Web Application Security Project (OWASP).

In addition, we have implemented an external development monitoring and control policy that recommends execution procedures, existing security measures as well as mandatory instructions for log management, access management, source code management and security testing during the development cycle.

15.2. Separation of development, testing and operational environments

Our development networks and infrastructures are physically and logically isolated according to the services provided. We also separate the various application environments such as development, testing, preproduction and production.

More specifically, the development environment is strictly restricted and only accessible to developers via our highly secure internal network.

16. Supplier relationship

We have processes and procedures in place to manage potential information security risks arising from the use of our products or services with specific vendors.

Furthermore, we carefully ensure that appropriate information security requirements are in place and agreed upon with each of our suppliers.

In addition, we regularly review, assess and proactively manage changes to the information security practices of our respective suppliers and service providers.

17. Vulnerability and incident management

17.1. Vulnerability management

A workflow has been set up for the production teams to manage CVE-type vulnerabilities using in-house tools and technology monitoring.

Various in-house tools enable automated tracking, monitoring and scanning of vulnerabilities that may affect our information systems.

An internal SLA (service level agreement) has been implemented to handle vulnerability reports, with a response time set according to the severity of the vulnerabilities identified.

17.2. Vulnerability scanner

Analyses are regularly carried out on several Infomaniak IP address ranges that we have specified. We are alerted via a dashboard when vulnerabilities are detected and programme action plans to quickly correct any vulnerabilities discovered.

17.3. Bug bounty programme

We actively collaborate with a community of researchers and ethical “hackers” to provide our clients with the highest level of security. A public programme is available as well as private programmes to test all the services offered to our clients.

Whistleblowers are adequately protected, while our employees have the possibility of reporting any suspected irregularities confidentially and anonymously at any time.

17.4. Security incident management

A well-established security incident management procedure clearly defines roles, responsibilities, the triage process, communication, response and mitigation, as well as the overall workflow required to ensure a complete resolution of the incident.

Depending on the severity and nature of the incident, Infomaniak Network may collaborate actively with the competent authorities and coordinate the incident handling process in order to ensure that it is resolved quickly and efficiently.

17.5. Crisis management

A specific crisis management procedure is formalised. This procedure outlines the different steps to be taken to resolve the incident as effectively as possible and to communicate the cause and impacts in the best possible way, both internally and externally.

18. Business continuity management

18.1. Steering continuity

A continuity plan is defined for the management and steering of the infrastructure services and assets of our data centers.

18.2. BCP and resilience

Business continuity is taken into account from the design and architecture phase of the services managed by Infomaniak Network.

Redundancy between our various data centers, as well as backups on multiple media and in several of our data centers, help ensure business continuity for our customers.

Disaster recovery solutions for our managed services depend on technical and software architectures and are tailored to the level of each business offering, based on specific constraints and production teams.

18.3. Business impact assessment

A business impact analysis (BIA) has been implemented to collect data in order to effectively plan and manage security incidents affecting our information system assets.

This BIA identifies key business activities and resources, as well as various levels of severity associated with them. Specific measures have also been defined to ensure business continuity in the event of an incident.

18.4. RPO and RTO

Infomaniak Network has established a continuity strategy taking three key factors into account:

- the Maximum Acceptable Disruption Time, also known as Recovery Time Objective (RTO);
- Maximum Acceptable Data Loss, also known as Recovery Point Objective (RPO);

- Potential financial and commercial impacts.

Where relevant, they are recorded in the business impact analysis (BIA).

18.5. Test plan

A test plan, which takes risk situations into account, is established and implemented annually. It allows for the following:

- upstream: measure the effectiveness of the plan in relation to the objectives of continuity, through indicators, audits, etc.
- during a crisis: monitor the actual service levels achieved and the functioning of the BCP operational procedures.
- A posteriori: to implement an improvement plan.

19. Compliance

19.1. Standards and regulations

19.1.1. ISO 27001

The Infomaniak Network teams rely on internationally recognised security standards, such as ISO 27001:2022 and ISO 27002:2022, as benchmarks for developing and managing the services they offer their customers.

These standards provide a robust framework to ensure the confidentiality, integrity and availability of sensitive information, as well as to manage information security risks effectively.

19.1.2. FADP and GDPR

Infomaniak Network has implemented a data privacy policy, which can be consulted on its website at the following address: https://www.infomaniak.com/en/legal/confidentiality-policy

In addition, the policy on the use of cookies can be accessed via this link: https://www.infomaniak.com/en/legal/policy-use-cookies

19.2. Audit

19.2.1. Internal audit

The monitoring of security activities within the scope of the Infomaniak Network certification is carried out by qualified consultants, who work under the supervision of the compliance team.

These consultants regularly review the items associated with the certified perimeters, in accordance with the audit plan and Infomaniak Network's declaration of applicability.

Documents relating to internal audits are confidential and may not be disclosed.

19.2.2. External audit

As part of ISO 27001:202 certification, the Infomaniak Network is audited annually by the certifying bodies.

19.2.3. Technical audit

Infomaniak Network calls on qualified experts to carry out regular technical audits of its information system and, as required, to implement new services.

19.2.4. Customer audit

Customers have the opportunity to perform penetration tests (pentests) on the services they use, in strict compliance with the terms and conditions specified in their contract.

They must also take into account the constraints of internal teams, such as only conducting pentests during office hours and informing production teams in advance.