Information Systems Security Policy
QP 16 601
Publication 6

Confidentiality

Level	Confidentiality	Checked level
0	Unclassified - Public information	X
1	Restricted - Invoke personnel only	
2	Confidential - Authorized users only	
3	Secret - Authorized users only	
4	Top Secret - Authorized users only	

Version

Date	Versions	Author(s)	Validated (V) / Approved (A) by	Version
21/01/2016	Publ. 1	SV	Security Committee	Original version
22/03/2017	Publ. 2	SV	Security Committee	Amendment to rule 9.2.3
28/06/2018	Publ. 3	SV	Security Committee	Addition of rule 9.10.6 and paragraph 9.16
10/07/2019	Publ. 4	SV	Security Committee	Amendment to: • paragraph 2, • terms, • rule 9.14.4, • paragraph 9.16
17/07/2020	Publ. 5	SV	Security Committee	Amendment to paragraph 7 and addition of paragraph 9.17
25/06/2021	Publ. 6	SV	Security Committee	Review

TABLE OF CONTENTS

1 - Subject ... 3
2 - Policy Overview ... 3
3 - Strategic Planning ... 4
4 - Perimeter ... 4
5 - Threat prevention ... 5
6 - CIAT and Classification ... 5
7 - Roles and Responsibilities ... 7
  7.1 - Security Incident ... 7
  7.2 - Roles ... 7
8 - Crisis Management ... 7
9 - IS security: Rules and Regulations ... 8
  9.1 - Security Policy ... 8
  9.2 - Asset management ... 8
  9.3 - Human Resources ... 9
  9.4 - Physical and Environmental Security ... 10
  9.5 - Protection of digital and hardcopy documents ... 10
  9.6 - Operating procedures and responsibility ... 11
  9.7 - Operational Security ... 11
  9.8 - Computer abuse prevention ... 12
  9.9 - Backup ... 13
  9.10 - Equipment and Information security ... 13
  9.11 - Access control ... 14
  9.12 - Information System acquisition, development and maintenance ... 15
  9.13 - Incident management ... 16
  9.14 - IT service continuity management ... 16
  9.15 - Compliance ... 17
  9.16 - Personal data ... 17
  9.17 - Cryptography ... 18

1 - Subject

These Invoke Information Systems Security policies cover a wide range of security issues, and are based on the Guide to Information Systems Security Policy created by the French National Information System Security Agency (ANSSI).

This document was drafted and validated by Invoke's Security Committee. The Security Committee was created with the purpose of setting security requirements, and addressing a variety of security issues faced by the company and its subsidiaries. Its members are thus tasked with preventing, detecting and responding to a security breach, whether on assets (data, servers, equipment, networks, etc.), or any other part of the company's business operations.

2 - Policy Overview

The protection of sensitive data is paramount to company business operations and reputation.

'Sensitive data' covers:

- Intellectual property, including the source code for all software (patented or patent pending), development processes, documentation and expertise acquired over the years;
- Client information, through Invoke's SaaS 'Software as a Service' hosting solution, Professional Services and/or Support (hotline);
- Information owned by or in any way related to the company's clients, partners or any other entity involved with the company's business operations;
- Information pertaining to employees, clients and third parties (administrative files or employee performance reports). The disclosure of such information would constitute an invasion of privacy;
- Data or information related to employees, temporary workers, interns, or people on work-study programs hereinafter jointly called Employees. The disclosure of such information would constitute an invasion of privacy;
- Data protection, which depends on a complex organizational context:
  - Geographical location (offices in multiple locations across western Europe);
  - Heterogeneous computing, such as software and other technology that increases efficiency (internal and external communications);

  - Heterogeneous environments (tests, material, equipment, etc.) needed by Invoke personnel in the performance of their duties;

3 - Strategic Planning

The strategy governing Information System Security applies to two types of data: production data and test data.

This distinction means that production data must remain available to its owner, who then decides whether to publish it. To the contrary, test data may only be used internally, unless otherwise stated by data owners during the implementation of resources.

Securing production and test data increases productivity and improves communications while preventing data overprotection. It also serves as an additional layer of security for data that may require increased security.

4 - Perimeter

This Information Systems Security Policy (ISSP) applies to both domestic and international business operations conducted by Invoke and its subsidiaries.

The security perimeter encompasses all human, technical, and logistical resource storing or processing data, regardless of its format (digital, hard copy documents, hand written notes etc.).

The security perimeter applies to:

- Persons authorized to access, use or process information through the company's information system;
- Invoke Employees and entities;
- Any third party using Invoke's information systems;
- Any and all data, regardless of the device/medium used to store or send information;
- Equipment, software and related component(s), including but not limited to:
  - Applications, processes and databases, and their hosting servers;
  - Communication networks;
  - Technical environments and any resource used to ensure proper equipment functioning;
  - Offices and facilities hosting IT/human resources;

5 - Threat prevention

Information System Security is essential to the protection of the company and any entity involved with its business operations. This is done by identifying what needs to be protected, assessing the risks associated with the use of a particular resource, and implementing security measures to counter potential threats. The Information Systems Security Policy focuses on a wide range of threats, including:

- Cyberattacks (intrusions, theft, deletion, system failure, denial of service, etc.), which may harm the company and result in a breach of contract;
- Information disclosure or loss of confidentiality, which may have a negative impact on:
  - Invoke data, namely the company's competitive edge (expertise, intellectual property, strategic development, etc.);
  - The company's clients, and their business operations or reputation (through the disclosure of financial information or strategic goals);
- Data edits, which may impact product and/or service quality, and result in the submission of erroneous reports or declarations for hosted clients;

6 - CIAT and Classification

Information security relies on the following:

- **Confidentiality:** ensure that information (files, messages, application, services, etc.) are accessed by authorized users;
- **Integrity**: ensure that data is an accurate and unchanged representation of the original secure information;
- **Availability**: ensure that information can be accessed by authorized users at all times;
- **Traceability**: ensure that any access or attempt to access information is recorded and that such record may be accessible by authorized users at all times;

Assets are assigned a priority level based on CIAT criteria. Priority levels range from 0 to 4.

PRIORITY LEVEL	Confidentiality	Integrity	Availability	Traceability
0	Unclassified Public information	N/A	N/A	N/A
1	Restricted Invoke personnel only	Low level	Non critical	Recommended
2	Confidential Authorized users only	Mid-level	Does not exceed 1 week	Highly recommended
3	Secret Authorized users only	Important	Does not exceed 24 hours	Required
4	Top Secret Authorized users only	No loss of integrity	Does not exceed 4 hours	Full traceability

The following must be considered when assessing priority levels:

- Maximum Tolerable Period of Disruption (MTPOD): refers to the duration after which the company's viability will be irrevocably threatened if a product or service delivery cannot be resumed.
- Maximum Tolerable Data Loss (MTDL): refers to the maximum loss of information (electronic and other data) which the company can tolerate. The age of the data could make operational recovery impossible or the value of the lost data is so substantial as to put business viability at risk.
- Retention: refers to the amount of time during which data can be restored, if needed.
- System Owner: refers to the person tasked with safeguarding an asset, granting access and assigning a priority level to such asset.

7 - Roles and Responsibilities

7.1 - Security Incident

A security incident is an event that affects the availability, confidentiality or integrity of an asset. Examples of such events include illegal use of passwords, computer equipment theft, hacking of files or applications, etc.

In the case of Invoke, a security incident can involve a company's proprietary data but also third parties' data (partners, clients, etc.). Regardless of the asset impacted, all security incidents are handled in a consistent manner by the company's executive management and internal teams.

7.2 - Roles

The roles

- The Security Committee is tasked with:
    - Drafting and sending out the Information Systems Security Policy and related documents, to Employees, contractors and any third party involved with the company's business operations;
    - Managing any issue or incident related to information system security;
- Heads of Departments must:
    - Read, understand and agree to abide by the terms of the ISSP;
    - Ensure that employees follow rules and regulations;
    - Report any incident to the Security Committee;
- Employees must:
    - Read, understand and agree to abide by the terms of the ISSP;
    - Report any suspected or actual incident to their superiors;

8 - Crisis Management

The Security Committee oversees all aspects of crisis management. To ensure that information is not compromised, employees must report incidents to a member of the Security Committee, either in person or over the phone.

Upon receiving a report of an actual or suspected incident, and depending on the seriousness of such incident, the Security Committee may set up a crisis management meeting and produce a communication plan and/or take swift action to ensure the incident is resolved.

Should a security incident occur on an asset classified Confidentiality Level 3 or above, owners will be informed of both the occurrence of the incident and the response plan adopted.

9 - IS security: Rules and Regulations

9.1 - Security Policy

GOALS:

- Draft, publish, and periodically update the Information Systems Security Policy, in compliance with Industry standards and European regulations;

POLICIES:

9.1.1 The ISSP is approved by the Security Committee and sent to all Employees and relevant third parties;

9.1.2 The ISSP applies to users of the company's Information Systems;

9.1.3 The company's Security Committee reviews, updates and validates the ISSP annually;

9.1.4 The Security Committee must review the ISSP every time a company restructuring occurs, or whenever a change is made to a technical environment;

9.1.5 Any change made to the ISSP will result in procedural adjustments;

9.2 - Asset management

GOALS:

- Identify assets and proceed to a detailed inventory of Information Systems;
- Identify assets and proceed to a detailed inventory of company data, with particular attention given to sensitive information;

POLICIES:

9.2.1 A detailed inventory of company assets must be completed, updated periodically, and remain available for consultation on company networks;

9.2.2 Installation of applications is subject to prior approval by the DSI. In addition, applications installed on workstations must be monitored and controlled;

9.2.3 Borrowers must be identified, along with the person (or his/her substitute when he/she is not available) in charge of ensuring that such equipment is secured, and that systems and applications are updated whenever necessary;

9.2.4 Assets are assigned a security classification based on security needs, according to CIAT (see above);

9.2.5 Borrowers must review the classification of equipment on loan, and are responsible for granting access rights;

9.3 - Human Resources

GOALS:

- Ensure that users follow the policies laid out in the ISSP;
- Reduce the risk of incident(s), errors and/or malicious acts through the implementation of Information Systems security measures. This applies to new recruits, current employees and departing employees;
- Ensure that security procedures are in place for departing Employees or Employees transitioning to other roles within the company;

POLICIES:

9.3.1 Employment contracts must include a confidentiality clause to provide legal protection against public disclosure of classified information;

9.3.2 Failure to abide by the Information Systems Security Policy may result in sanctions and penalties, such as disciplinary action. For more information, see Invoke’s Company Policy and Procedures;

9.3.3 The DSI releases periodical reports and updates to ensure that users stay informed on information systems security issues.

9.3.4 The procedure implemented by the DSI for departing employees or employees transferring to other positions includes:

- Revoking user permissions;
- Collecting any and all equipment borrowed;
- Deleting or archiving all departing employee data stored on company equipment and network(s), or reassign such data to replacement(s);

9.3.5 A procedure is in place to allow executives to access an employee’s personal data (such as files, and electronic communications) if such an employee is unable to perform the tasks required;

Employee access to confidential information is restricted, regulated and subject to prior approval by owners;

9.4 - Physical and Environmental Security

GOALS:

- Ensure that access to company facilities and technical environments is restricted;

Policies:

9.4.1 Access to company facilities is restricted to authorized personnel. Company issued passes and keys provide access to offices and facilities. Employees are only granted access to rooms and facilities that are necessary for the performance of their duties;

9.4.2 Visitors must be accompanied by authorized personnel at all times. Authorized personnel may be liable for any and all action taken by visitors while on company property;

9.4.3 The DSI manages access to technical environments;

9.5 - Protection of digital and hardcopy documents

GOALS:

- Ensure that sensitive data is stored securely and remains available;
- Ensure that servers and server room security is homogeneous (fire, humidity, overheating, flooding, etc.);

POLICIES:

9.5.1 Hardcopy documents are kept in secure locations to protect against the risk of theft, fire, humidity, flooding, etc.;

9.5.2 Computing equipment is kept in secure locations. Preventive/protective measures are in place to ensure that sensitive equipment is protected against the risk of fire, overheating, or power outage. Such measures are relative to the level of sensitivity of each piece of equipment;

9.5.3 Internal teams conduct periodical reassessments of physical security procedures. This may be done in cooperation with contractors;

9.5.4 Repairs and the exchange of sensitive equipment (containing sensitive data) is subject to contractual obligations. Contracts lay out conditions surrounding all types of interventions by contractors, such as maximum timeframes and the protection of Integrity and Availability of sensitive data;

9.6 - Operating procedures and responsibility

GOALS:

- Ensure that information system processes remain operational and secure;

POLICIES:

9.6.1 The DSI oversees the creation, management, and dissemination of operating procedures (systems, networks, workstations, applications), and assigns responsibilities (monitoring, approval, updates);

9.6.2 Information system documentation (architecture, operations and procedures) is backed up and its access is restricted;

9.6.3 Any action taken on assets (updates, parameters, errors, fixes, etc.) is processed through the request management system and thus fully traceable;

9.6.4 DSI executives complete a risk assessment analysis prior to validating major modifications made to information systems (external access rights, architecture, critical applications);

9.7 - Operational Security

GOALS:

- Monitor system events;
- Ensure information systems are operational;
- Detect and respond to malfunctioning equipment/systems;

POLICIES:

9.7.1 Information Systems equipment is monitored in real time, and at all times. Information related to the condition of equipment, service availability and resources is updated constantly. IT Department executives are notified in the event of a technical incident, and may open a ticket on the request management system;

9.7.2 System Traceability (logs) must be activated wherever possible and whenever it is deemed relevant;

9.7.3 Logs must be collected and stored for at least 180 days (sensitive assets) to be able to provide clear evidence of user action;

9.7.4 A procedure is in place to manage corrective and security updates on all system equipment, networks, work stations and applications;

9.7.5 Teams handling equipment or systems deemed obsolete must identify such equipment and systems, and provide the DSI with a risk analysis;

9.8 - Computer abuse prevention

GOALS:

- Protect software and information integrity;
- Control and filter internet access;

POLICIES:

9.8.1 Servers and workstations must be protected, and their access supervised to protect information integrity (data, configuration, etc.);

9.8.2 Authorized and non-authorized network protocols must be identified and implemented on perimeter security equipment, as well as on internal networks, so as to enable partitioning;

9.8.3 Remote connections to company tools must use stream cyphers;

9.8.4 Authentication (ID and password) must be encrypted to protect the company against data interception;

9.8.5 The DSI keeps a list of authorized input and output flows. Flows not mentioned in this document are not authorized;

9.8.6 Internet connections are filtered and logged. Access to certain sites is restricted. A list of restricted sites is frequently updated;

9.9 - Backup

GOALS:

- Maintain Information integrity and availability, and ensure recovery;

POLICIES:

9.9.1 Backup policy is in place to ensure system backups and data recovery. This policy covers:

- Backup administrators;
- Frequency and type of backup (full, incremental, differential);
- Equipment (tape, disk);
- Duration of data retention;
- Periodicity of restoration tests;

9.9.2 Data must be stored in secure locations, away from the production environment;

9.9.3 DSI executives and technical teams must review and update this backup policy periodically;

9.9.4 Employees must back up data onto available storage space, and must not resort to the use of external storage (public clouds, flash drives, etc.);

9.10 - Equipment and Information security

GOALS:

- Ensure the information stored or shared (internally and externally) remains confidential;
- Prevent unauthorized disclosure, modification, or deletion of information;

POLICIES:

9.10.1 Data owners approve access permissions (read, or read and write);

9.10.2 Users must follow best practices with regards to sensitive data management. For instance, users must:

- Store sensitive data on secure devices/in secure locations;
- Use a shredder to destroy sensitive documents;
- Avoid leaving documents on and around printers, photocopy machines and fax machines;
- Store hardcopy documents in secure locations such as safes and locked file cabinets;

9.10.3 Users must not store sensitive information (internal or external documents) on mobile devices (laptops, flash drives, etc.), unless authorized to do so by data owners. The same applies to online storage, such as public clouds;

9.10.4 The DSI implemented a procedure to ensure that all equipment and accessories borrowed are returned, and that all data is deleted securely before lending equipment to other employees;

9.10.5 The DSI ensures that data stored on a piece of equipment is securely deleted prior to its disposal;

9.10.6 The DSI ensures that internal storage encryption is enabled on all mobile devices (laptops, tablets, etc.) and controls it.

9.11 - Access control

GOALS:

- Ensure controlled access to information;
- Monitor and control access to information systems;

POLICIES:

9.11.1 All users (including employees and third parties) connect to the network using a personal account, and are thus clearly identified;

9.11.2 Monitoring and traceability of user accounts (creation, use, modification, deletion) is essential;

9.11.3 Traceability applies to any and all access to Information Systems;

9.11.4 Records of user access to Information Systems must remain available. Such records may serve as evidence;

9.11.5 A procedure is in place for the position change process (new hires, departing employees and job transfers), and includes updating employee information and access rights;

9.11.6 Employees are required to use complex passwords to access Information Systems. This extra layer of security is mandatory and essential to information security. This includes:

- Password delivery method;
- Complexity: minimum length, use of different types of characters;
- New passwords, every time the DSI requires a password change;
- Limits on attempts to access user accounts;
- Auto lock;
- Password expiration. New passwords are required periodically;

9.11.7 Information security relies on a range of systems in place:

- Auto lock after a period of inactivity;
- Employees must lock their computer before leaving their workstation;

9.12 - Information System acquisition, development and maintenance

GOALS:

- Ensure security management throughout the system life cycle;
- Reduce the risks associated with the use of technical and application vulnerabilities;

POLICIES:

9.12.1 Developments and acquisitions must take into account a range of security needs. DSI executives assess security needs based on information classification (see: 6 - Security Needs);

9.12.2 Vulnerability audits are conducted on applications, databases and systems:

- From the time they are implemented;
- Periodically;

    - In the event of a major change to the operating system, application or manual configuration;
    - Whenever a new, major vulnerability is discovered (in order to approve or reject operation);

9.12.3 The implementation of a system or application requires the creation of several environments and their separation (development, validation, production);

9.13 - Incident management

GOALS:

- Implement an efficient incident management policy to ensure information security;
- Ensure employees report any incident and security breach;
- Ensure preventive and/or corrective action;

POLICIES:

9.13.1 Employees witnessing or suspecting a security breach on workstations (worms, viruses, Trojan horses) are required to know and follow procedures;

9.13.2 Systems, alerts and vulnerabilities are constantly being monitored to ensure information security;

9.13.3 Indicators are used to keep a record of incidents, specifically their origin, cause, impact on confidentiality, integrity, availability, and traceability;

9.13.4 DSI executives analyze security incidents carefully. This results in the creation of response plans that include improved (preventive or corrective) measures, and/or lead to the implementation of new measures;

9.14 - IT service continuity management

GOALS:

- Ensure system backup in the event of a minor incident (equipment malfunction);
- Ensure IT service continuity in the event of a major incident. This includes a timely response to an incident on a server room;

POLICIES:

9.14.1 New projects must take into account system backup requirements, namely the Maximum Tolerable Period of Disruption (MTPOD) and the Maximum Tolerable Data Loss (MTDL);

9.14.2 DSI personnel is tasked with creating system backup plans based on past incidents;

9.14.3 DSI personnel must test system backup procedures and solutions periodically;

9.14.4 An IT Service Continuity Plan (ISCP) is drafted to ensure proper response to major issues impacting a server room (power outage, fire, etc.) and is part of the security documentation;

9.14.5 Service continuity drills are scheduled annually;

9.15 - Compliance

GOALS:

- Prevent a security breach, a breach of intellectual property, and a breach of contract;

POLICIES:

9.15.1 The Security Committee ensures that employees comply with the rules and regulations laid out in the ISSP;

9.15.2 The DSI may use non-intrusive software tools on workstations and servers to ensure that employees comply with ISSP rules and regulations;

9.15.3 The DSI conducts inventories and follow up on the installation of software requiring a user license;

9.15.4 The DSI ensures that the number of authorized users for any given software does not exceed the number of licenses purchased;

9.15.5 Any and all software created by a member of the workforce is the property of Invoke, as stipulated in employee contracts and internship agreements;

9.16 - Personal data

GOALS:

- Adopt a consistent policy for personal data storage and processing based on the European General Data Protection Regulation (GDPR) in order to meet its new obligations as:
  - The data controller of Invoke's business functioning data;
  - A contractor regarding all the activities and services provided to its clients.

POLICIES:

9.16.1 Any processing of personal data is identified;

9.16.2 The collection of personal data is limited to the data necessary for the processing being carried out;

9.16.3 Personal data is not stored longer than required by the processing carried out;

9.16.4 Any request to access, modify or delete personal data controlled by Invoke will be processed within one month of receipt;

9.16.5 Personal data is not stored or transferred outside the European Union;

9.16.6 Personal data protection results in several specific documents:

- Personal data protection regarding Invoke's SaaS hosting services, Professional Services and Support;
- Information to Employees;
- Personal data protection requested to contractors when Invoke is the Data processing controller.

9.17 - Cryptography

GOALS:

- Ensure a secure network transit consistent with business and confidentiality goals;
- Define an encryption key management policy.

POLICIES:

9.17.1 Storage devices for laptops must use a reliable encryption system, that is managed and controlled centrally.

9.17.2 Any non-compliance or failure of the encryption must be notified to the IT department and must be handled as a security incident.

9.17.3 Access to encryption keys must be restricted to authorized personnel only, for whom access is necessary to perform their functions.

9.17.4 Any encryption key revealed must be revoked and replaced immediately.

9.17.5 Sensitive data transmitted across networks (public or internal) must be encrypted.

9.17.6 Only protocols, algorithms and cipher suites that are up to date and that ensure highly secure exchanges must be used. If they do not comply with the state of the art, they must be disabled or a risk analysis must be conducted consequently.

9.17.7 Incoming or outgoing emails must be encrypted, partner servers permitting. Mandatory encryption must be ensured for some partners when exchanged data are too sensitive.

9.17.8 Access by a third party (client, partner, etc.) to a resource hosted by Invoke through public networks must be secured by using certificates issued by a trusted recognized authority.