**SBS**

# Security Management Plan

Edition, Maintenance and Support

Version 2025.1

Status : Validated 23/05/2025

# 1. Presentation of the Security Management Plan

This Security Management Plan (“SMP”) describes the security measures, the organization and the processes put in place by SBS as part of the software edition activities, providing support and maintenance to each customer. All capitalized terms not defined in this SMP will have the meaning given to them in other parts of the Agreement.

This document describes the dispositions applying on disponibility, authenticity, integrity and confidentiality regarding data protection, including Personal Data.

# 2. Reversibility clause

SBS ensures compliance with the SMP and the security levels during the duration of the Agreement and the reversibility phase. Any data transfer requires prior validation from the SBS ISO and the security contact of the Customer.

# 3. Security Audits

SBS conducts regular security audits, tailored to the each product line or service line and to a specific scope. These audits may include technical assessments, external evaluations, and penetration testing.
The Customer may conduct audits at its own expense, in accordance with the conditions set out in the General Terms and Conditions (GTCs) and Specific Terms and Conditions (STCs).

# 4. Global Security Clause

SBS is responsible for the security procedures of its subcontractors

# 5. Security Organization

## 5.1. Information Security Policy (ISP)

The SBS’s Information Security Policy (ISP) is managed by the SBS CISO.
The SBS’s ISP is available to all employees via the intranet.
The ISP may be presented during audits carried out by the Customer.

## 5.2. Security committee

SBS has implemented an internal security committee which takes place on a regular basis within the product and service lines. The purpose of the internal security committee is to control the application of the SMP by presenting security KPIs and key information.
Depending on the options/services subscribed by the Customer, a customer security committee will take place at regular periods.

## 5.3. Customer organization

The Customer has the obligation to appoint a security contact in charge of applying Customer’s information security policy. He will be the privileged point of contact for SBS on security matters and the point of contact for security audits, distribution of security documentation or other security topics and security committees. In case of a security incident or threat, she or he will be the contact person for the various exchanges and follow-ups. The contact details of Customer’s security contact and the Data Protection Officer must be shared with SBS.

## 5.4. SBS Security department organization

**Objective.** The objective is to define a governance for implementing and verifying the Information Security Policy of SBS (ISP).

**SBS CISO.** The SBS CISO is appointed by the SBS management.

**Information Security Officer of the product or service line.** The Information Security Officer (ISO) assigned specifically to the product line or support service line is responsible of the security in the contract. The roles of CISO and ISO are defined in the dedicated function sheets validated by the yearly security organization note issued by the SBS CISO.

### 5.5. Mission of the security department

The security department's organization is reviewed by the SBS CISO on a yearly basis. The result of this review is published internally to inform the different stakeholders of the roles, the mission, and the security objectives to be reached for the current year. The security department's mission is to:

- Ensure the operational application of the Information Security Policy (SBS ISP) and to report any discrepancies (in its application or unsuitability to the activities of SBS)
- Manage security risks and initiate actions to prevent crisis and make SBS more resilient in case of a crisis
- Help setting up the necessary means at each Business Unit (BU) level to achieve the yearly SBS security objectives
- Make employees aware of security issues
- Formalize and deploy the yearly security control plan and support the actions identified following the review
- Tracking the coverage of vulnerabilities in the SBS products and the associated remediation plans
- Participate actively to security communities
- Report all incidents and security issues.
- Carry out a security watch necesssary for the improvement of the security processes of SBS

All security roles and functions must be validated by the SBS CISO.

### 5.6. Risk management

Risk management is an integral part of the SBS security governance. It is carried out on an ongoing basis between the operational teams and the ISO. SBS has put in place a risk security exception process that manages deviations from the established security policies or the specific requirements from the product and services lines.

## 6. Human activities Security

### 6.1. Objectives

- Ensure that SBS employees are aware of their responsibilities and can perform their assigned functions in accordance with current regulations.
- Reduce the risk of theft, fraud, or misuse of computer equipment.
- Ensure that SBS employees are aware of threats to information security, personal or financial data, or other confidential Customer data.
- Reduce the risk of human error or malicious behaviour by applying the "four eyes" principle.
- Verify that the accounts and access rights of employees leaving the company are effectively deactivated. When an employee leaves the company, all rights are automatically revoked.
- Ensure that the access rights are regularly reviewed.

### 6.2. Security awareness and training

All employees are regularly trained and made aware of security in their context. They apply the "clean desk policy". An information security awareness program defines security requirements. The management sponsors the implementation of this program.
Employees accessing SBS or its customers' data are particularly sensitive to: (i) the confidentiality of the data processed, (ii) the ethics of the company to which the service relates, (iii) social engineering, and (iv) damage to the image and reputation of SBS or its customers.

### 6.3. Security measures

**Recruitment.** During recruitment, the HR department performs controls depending on the legislation and the rules of the country of the new employee.

**Confidentiality clause**. SBS undertakes that a confidentiality clause is systematically included in the employment contract of its employees. The information covered by the confidentiality clause and the prohibition of disclosure mainly concerns: (i) hosted content: the information or functions processed by the system, (ii) information whose disclosure could compromise the security of the system (passwords, encryption keys, documentation on the architecture and security of the system, etc.), (iii) Customer's personal, or confidential information, (iv) exposure of Customer's name in unrestricted spaces, (v) depending on the scope of the services, additional clauses may be implemented.

**Training and awareness**. SBS is committed to ensuring that its employees receive appropriate awareness and regular updates on security requirements related to the regulations of the services provided, the control measures, and specifically the data management. For SBS employees, SBS implements the SBS security training program.

Through its training university, it ensures a basic level of security awareness for all its employees. The training covers the following topics: (i) Security basics for everyone, (ii) Security in development (training provided based on the employee's role/function), (iii) Data protection, (iv) Annual phishing prevention test campaign.

**Termination or modification of the employment contract**. Any SBS employee or subcontractor who ceases to work will have all their access rights revoked. The specific access rights for administrators will also be cut off.

# 7. Assets security

## 7.1. Objective

Define, implement, and maintain appropriate technical measures to protect information system assets against threats from identified risks.

## 7.2. SBS requirements

The different configurations of the workstations, which, in function of the service, connect to the information system or to the platform, are described and qualified.
The rules of classification of information (meeting minutes, documents, reference documents, databases, data files, emails, etc.) from SBS or from customers are identified and applied (see chapter Classification of information).
All the equipment that makes up the information system, the SBS workstations and the infrastructure for the provision of the Services have an up-to-date virus protection software.
The update (recovery and distribution) of the signature bases and anti-virus softwares is carried out on the workstations and the servers at the time of publication by the editors.

## 7.3. Security measures of the workplace

### 7.3.1. Laptops

The workstations used by the SBS teams are provided by the IT Department and therefore comply with the patch management policy in terms of “anti-virus” coverage and the application of Windows security patches.
The mastering of workstations is carried out by the IT department, as well as the processes for providing, recycling, and destroying workstations.
The workstations are always in a maintained version of Microsoft Windows and have by default a hard disk encryption tool.
Each employee must lock their screen when leaving their workstation or when it is left unattended. By default, the screen locks after a few minutes of inactivity to prevent theft or data loss.

The use of non-standard resources (BYOD) is not permitted to access our customers' production environments.

### 7.3.2. Microsoft Office 365

The collaborative and messaging tools used are provided through the cloud version of Microsoft, managed by the IT department. The messaging system includes antivirus and anti-spam security solutions, which help reduce the risk of virus propagation.
Exchanges with customers by email must respect the SBS’s information classification rules and the Customer’s rules of use.
SBS allows its employees to have an email access on their professional or personal phone.
In all cases, the encryption of the Outlook database is automatic. It is controlled by a MDM (Mobile Device Management) processes.
By default, the SBS messaging gateways use the TLS 1.2 protocol, which enables encryption of transported messages. If the Customer’s gateway does not accept the SBS’s encryption level, no message will be sent until a secure method has been agreed.

### 7.3.3. Mobility

Employees may telework according to the provisions implemented by SBS.
In this case, they must respect the SBS directives and follow the different security rules defined in the directives.
A sanity check is performed to control the compliance of the employee’s workstation (example: antivirus installed and up to date, Windows updates installed, …) before launching the VPN connection to the SBS network.

### 7.3.4. External media

SBS ensure the confidentiality of external physical media required for the services requested by the Customer: paper media if necessary.

#### 7.3.5. Operations asset database

SBS undertakes to ensure that all IT or other assets (documents, various materials) essentials to its activity and the delivery of services are protected in accordance with the rules of the Information Security Policy.
The assets are inventoried and managed by product, adapted to the context, and the security follow-up of those assets (obsolescence for exemple) is ensured by the ISO of each product.

### 7.4. Classification of information

The classification levels are as follows:

**C1 Public:** A record with non-sensitive, non-confidential information is considered unclassified or public.
**C2 Restricted use** (Limited to need-to-know): default classification for all new documents.
**C3 Confidential:** Disclosure to an unauthorized internal or external third party may cause harm to SBS, customers and partners or employees.
**C4 Strictly confidential:** Disclosure may cause serious harm to SBS and its customers.

### 7.5. Protection related to the handling of information

The employees of SBS apply several internal rules mentioned below:

- In the employment contract for compliance with legal and regulatory requirements (GDPR, Labor Agreement, internal policies, IT charter, etc.),
- In the IT department's guides and instructions for network and equipment security,
- In the Documentation Management Guide for document classification, which describes different use cases,
- For assets managed by the IT Department, the integrity of data in the Information Systems access logs is the responsibility of the IT Department administrators.

Shredding of information:

When information is no longer needed, means are made available to SBS employees to destroy it, for example:

- Shredder of paper,
- A procedure is deployed by the IT Department for the decommissioning, the disposal and the destruction of the equipments.

## 8. Logical security

### 8.1. Security requirements

- All connections to the SBS Information System (IS) on which SBS is providing the Services to its customers, are subject to procedures (editor support activities, third party subcontractors),
- All connections made by Infrastructure administrators (IM) to the SBS Information System (IS) on which SBS is providing the Services to its customers, are tracked, protected, and archived in an integrated manner over a sliding period,
- In case of a data leakage or incident, the generated traces can be investigated for detecting the involved parties and the used resources,
- Logical access rights are subject to a control procedure: any change in status (arrival, departure, change, etc.) must be considered. The access rights must be modified accordingly,
- Users must be attached to a profile related to their function,
- Users are automatically forced to change their passwords at least every 90 days, including privileged users.

### 8.2. Internal user account management

#### 8.2.1. Rules regarding internal user accounts

For all access to SBS's services, tools or applications, SBS employees follow the SBS request management process (ITSM request management application).
The following SBS rules are applied:

- An SBS employee has a unique and personal identifier,
- It is authenticated with the Active Directory. Its access to the various systems depends directly on the rights contained therein,
- At the start, the employee has at least an MS Office account, an Internet access, a mailbox, password protected,

- He has only access to necessary applications to accomplish his missions,
- Certain employees have privileges to carry out administration, maintenance, or upgrades to systems and applications; their number are reduced to the strict minimum and privileges are reviewed regularly. Those users use a strong authentication,
- A password management policy is defined and applied,
- Passwords must comply with SBS's password policy,
- The IT policy prohibits the employee from disclosing his authentication information,
- The access rights of employees are not transferable,
- The access to the system is slowed then blocked after a certain number of failed authentication attempts, as defined in the ISP,
- When an employee leaves the company, he loses all his access rights automatically
- The users are automatically disconnected after a certain inactivity period,
- Avoid generic accounts. If the use of generic accounts cannot be avoided, trace files allow for logging the activities performed by the users by means of these generic accounts,
- Systematically change the accounts provided by default by manufacturers and editors,
- Generate and store passwords in a secure manner.

#### 8.2.2. Access rights management for internal users

Assigning / changing access rights:

- Requests to create or modify access rights to specific applications and services are subject to validation by the hierarchical manager (or the application manager).
- Logical access rights are granted according to the needs of the employee and his function. The granting of these rights is systematically tracked.

#### 8.2.3. Access rights removal for people at the end of contract

As soon as an employee leaves the company, internal company procedures are applied and all access rights to company applications are removed. The default offboarding process is launched on the next day.

#### 8.2.4. Review of access rights

Access reviews are determined according to the roles (administrators, users, etc.).

### 8.3. Management of accounts on Customer environment

#### 8.3.1. Management of the access rights on customer's environments for support services

For Support activities, the access rights management of an employee of SBS on Customer's environment follows the Customer procedures and are under the responsibility of the latter.

### 8.4. Ticketing tool

#### 8.4.1. Authorizations

The ticketing tool has an authorization management system that allows each user to be assigned a profile. This profile will define the actions that can be performed on the tool (consultation of documentation, consultation of tickets, creation of tickets, administration, etc.).

#### 8.4.2. Authentication and password

Authentication for SBS users is based on Active Directory rules. The access modalities can evolve according to the needs expressed by SBS.

#### 8.4.3. Assigning / changing access rights

When a employee must use the ticketing tool, an account is created, and a profile is assigned to him according to his needs. An access rights review is executed on a regular basis.

#### 8.4.4. Withdrawal of access rights for people at the end of their contract

For SBS users, blocking the AD account will block access to the ticketing tool.
It is the responsibility of the Customer's point of contact to manage the onboarding and offboarding of the Customer's users and to submit the necessary requests to SBS.

# 9. Physical security

## 9.1. Physical Security on SBS premises

The organization in charge of management of the premises ensures that the services required in terms of general services (electricity, air conditioning, etc.), fire safety and anti-intrusion services comply with the standards and security requirements imposed by local regulations, insurance companies and the ISP:

- By default, the collaborators of each site use a badge access control system. This system is used to restrict access to premises to authorized persons only,
- If necessary, the premises are divided into zones to control access,
- Computer rooms (or technical rooms) have restricted access,
- According to the country, the site's internal regulations describe the security instructions on-site and are accessible to all site employees (via on-site display),
- The electrical emergency systems and air conditioning systems are sized according to the site and its criticality,
- The site can have remote surveillance of the site (e.g., access doors to the premises, windows on the ground floor, machine room doors, etc.),
- The management of physical access is the responsibility of the landlord's Site Manager and SBS's General Secretariat or its equivalent in other countries,
- Responsibility for people and assets is assigned to the Site Director, who is supported by the landlord's Site Manager.
- The Site Infrastructure Security Document (“SISD”) summarizes these requirements for each of the sites.

### 9.1.1. Objective

- Prevent unauthorized physical access, damage or intrusion into the premises.
- Prevent loss, damage, theft or compromise of assets and disruption of SBS operations.

### 9.1.2. Site Infrastructure Security Document (”SISD”) for the sites

SBS sites are managed either by 74Software, or directly by SBS, or by SBS’s landlord (SSG).

A site manager is assigned to each site; his role is implementing the site's security measures in accordance with the Information Security Policy.
A SISD (Site Infrastructure Security Document) is available at each site, under the responsibility of the site managers and general services.
The actions identified in the SISD and requirements set by the department include:

- Preventing unauthorized physical access, damages, or intrusions into the Service premises and information,
- Preventing data loss, damages, theft, or compromise of assets and the disruption of the Service operations.

# 10. Security incidents management

## 10.1. Objectives

Make sure that information security incident reporting procedures allow for early corrective action.
Implement consistent and effective policy and processes for managing information security incidents.
Make sure that a rapid reporting of all information security events through appropriate reporting channels is in place.

## 10.2. Security event

A security event is an event that attracts attention because it is potentially compromising the security of a system and its data.

## 10.3. Security Incident

After analysis, an event may be requalified as a security incident when the integrity, confidentiality or availability of information is potentially compromised in an undesirable or unauthorized manner. A security incident may require corrective actions, crisis management, incident reporting and post-incident evaluation.

## 10.4. Procedures

SBS applies the security incident management policy defined in the ISP. The latter specifies the escalation process, the people to be contacted and kept informed, and the formation of the crisis unit that will be activated in case of a major security incident. Given the nature of the information contained in this procedure, this document is confidential.

The security incident management process involves three levels:

- The local level, as soon as the incident is detected at operational level,
- The entity and site level, after escalation,
- The SBS level then 74 software after escalation.

The process for the follow-up of an incident is: Reporting, Collection of evidence, Analysis, Possible escalation, Processing, Communication, Post-incident analysis.

### 10.5. Declaration and follow-up

The ISO of the product or the service line is notified by the line teams of each security incident. For Support context, all information security incidents affecting SBS and the services subscribed by the Customer must be notified to the Customer within the regulatory timeframe (maximum 24 hours) following the qualification of these incidents by ISO.
A procedure exists and it is shared on request. The procedure contains information regarding the notification, descriptions, remediations and lessons learned.

It is possible to declare a security incident via the ticketing tool as well, if the security incident is considered as critical by SBS then it will be treated as a critical incident (P1).Timeframes regarding treatment of incidents are indicated in the Contract. In other cases, it will be handled by the product or service line's ISO as soon as possible.

In case of a security incident, SBS will apply all means for collaborating with the Customer's CISO, or the security contact designated, assuring a transparent communication and by actively participating in providing evidence required for the analysis and remediation of the security incident.
To contact SBS, a specific email address is provided: security.incident@sbs-software.com

### 10.6. Personal data incidents (GDPR)

The security incident management process includes the management of personal data breaches.
The incidents are reported to the SBS data controller as soon as possible and follows the regulatory requirements.
If the incident involves personal data, additional information must be communicated to the 74Software's DPO and the Customer's DPO if he is impacted.
The email of 74Software's DPO is GDPR.ACCESS@sbs-software.com

### 10.7. Report

All employees and contractors must report such problems to their manager as soon as possible to avoid information security incidents. Security incident reporting is done via the IT Service Management application, which has a dedicated process for security incidents.

## 11. Business Continuity Management

SBS has the organizational and technical means to ensure the continuity of activities of his Edition activities and the Services provided to his Customers.
SBS shall endeavour to maintain the level of service as defined in the Agreement and to protect critical business processes from the effects of an information system failure, and to ensure the recovery of these processes as soon as possible. In the case of an incident affecting the availability of the service, SBS undertakes to restore the Service as defined in the Agreement.
SBS maintains documents describing the measures of business continuity and a test is realised yearly with a report provided to the customer on simple demand.

## 12. Encryption

### 12.1. Objective

Ensure the correct use of encryption to protect the confidentiality, authenticity and/or integrity of information.

### 12.2. Requirements

A policy for using cryptographic measures to protect information has been developed and implemented by SBS.

### 12.3. Encryption at rest

Company laptop

All SBS workstations are encrypted at rest (the Solution deployed currently by the IT department is Bitlocker). SBS undertakes to use robust encryption protocols with no known vulnerabilities.

### 12.4. Encryption of data in transit

By default, an encrypted transfer protocol (sFTP, HTTPS, …) must be implemented for data exchange between SBS and his customers.
For encrypted communication flows, the TLS 1.2 is applied, or a higher version once it is validated by SBS.
This measure is mandatory when the Customer data are present in the environment.
A compensation measure can be the deployment of a VPN if the flow is not encrypted.

## 13. Security of service operations

### 13.1. Backups

As part of the Support activities, SBS undertakes to back up the necessary infrastructure for the run of the service with the Customer. SBS is responsible of the restoration, using the latest backup made, of every data, files or information lost or damaged.

### 13.2. Separation of environments

SBS R&D has its own development environments dedicated to each activity: tests, qualification, integration, …
As part of the Support activities, unless explicit Customer demand, production data are not copied in SBS environments.

### 13.3. Protection agains malwares

Antivirus and EDR are deployed on all SBS employee's workstations. Antivirus and EDR are deployed at least on all Windows OS, and some Linux environments.
Antivirus monitoring is conducted by the IT department. A monthly reporting of the security level of the computer park is presented in SBS security committee.

### 13.4. Logging and tracking

#### 13.4.1. Clock synchronization

For logging systems, a master clock ensures that all servers are synchronized on the same time base.

### 13.5. Vulnerability management on development infrastructure

#### 13.5.1. Criticality and CVSS scoring

Vulnerability handling is analyzed and reported, with an assessment based on raw CVSS 3 scoring:


The impact of vulnerabilities can vary, it can be recalculated automatically or manually depending on certain parameters such as the exposure of the concerned asset, its environment, ... Vulnerabilities considered as Critical (contextualized CVSS ≥9) and proven are considered like a P1 incident and addressed immediately.

#### 13.5.2. Vulnerability watch

The vulnerability watch service is organized in SBS and relies mainly on:

- CERT bulletins from the Sopra Steria Group's cyber security unit,
- A subscription with a private CERT.

The management of security patches applied to workstations and servers is carried out by the IT department and a monthly report on the workstations is made available to the CISO. For servers managed by operational teams, the same patch management obligation is imposed. In the event of a deviation, a security exception is handled by the security teams.

### 13.6. Connection to customer's environments

**Connections from SBS**

Exceptionally, as part of its Support activities, SBS may be required to connect to a Customer environment. In this case, the connection is secure, supervised by the Customer, temporary, limited in number of SBS employees and restricted to strictly necessary actions.

# 14. Development security

## 14.1. Software development

### 14.1.1. Security in development

SBS has created a software obsolescence policy and a secure development guide for its needs. This document provides a non-agnostic coding guide to protect SBS products from the threats listed in the OWASP[1] Top 10 framework. This document is applicable to all SBS products and it is enriched by additional documents.

Managing the obsolescence of third-party components and products, managing licenses for open-source software, and managing vulnerabilities are covered in specific chapters below.

### 14.1.2. Audits and security reviews

During the development and life of an SBS product, security audits and reviews are carried out:

- Statically through source code analysis ("4-eyes" review, Static Application Security Testing - SAST, Software Composition Analysis - SCA, Software Bill of Materials - SBOM) or dynamically through Application Security Audit - ASA, and penetration testing
- To verify that security policies have been respected during the development lifecycle,
- To identify all vulnerabilities that could lead to the exploitation of security vulnerabilities and identify remediation actions for them.

Vulnerability monitoring through the tracking of CERT bulletins is also integrated into the software development and the lifecycle of the softwares (see above).

### 14.1.3. Automatic analysis and deployment

Whenever possible, Software Composition Analysis (SCA) and Static Application Security Testing (SAST) tools are integrated into the continuous integration process of the product to ensure that new developments do not incorporate new vulnerabilities.

### 14.1.4. Vulnerability management

Each vulnerability is assigned a criticality level and a priority level.
Vulnerability treatment follows the remediation process defined below.

**Raw CVSS Vulnerability Score**

Criticality is calculated using the raw CVSS notation already presented earlier. The determination of criticality takes into account all criteria including the complexity of the attack, exploitation and the existence of remediation of the vulnerability. If for any reason the CVSS notation is not suitable, another standard validated by the SBS ISO community may be used.

**Criticality and priority after contextualization**

A vulnerability is contextualized exclusively by SBS, in terms of business impact, likelihood, and exploitation, to set a priority.

The correction, information to customers and delivery processes are tailored to the priority of the vulnerability. The remediation is primarily carried out on the most recent version and then in compliance with the Editor policy on the maintained versions.

**Vulnerabilities follow-up**

Vulnerabilities are traced and monitored by the ISO of the product or service line.

## 14.2. Secure Software Development Lifecycle

In accordance with best practices, all software versions are uniquely identified and tracked throughout their lifecycle; all changes are clearly associated with a single software version.

Managing changes during the software lifecycle ensures that all changes are identified, evaluated, and approved. A process is in place for the registration of requests, their justification, the analysis of their impact and the final decision. This includes approval by the responsible personnel, traceability of the people who created/modified the source code, and the possible execution of additional security tests before delivery.

Protecting the integrity of software throughout its lifecycle is a mature process. Mechanisms and tools are in place to protect the integrity of the source code and embedded third-party components; they make it possible to identify all the changes and the people affected by them.

Threats and vulnerabilities in the software design are identified and evaluated on an ongoing basis: a clear and mature process is in place to record the threat inventory and vulnerabilities, the outcome of assessments, remediation or mitigation decisions, and approvals; it is run regularly during the software lifecycle.

The purpose of vulnerability detection and mitigation is to ensure, through regular checks, that products developed by SBS do not contain any known critical or high vulnerabilities at the time of delivery to Customer. To do this, the entire codebase is analysed, including third-party, shared, and open-source components and libraries. Stakeholders are informed about potential security issues and mitigation options. Security updates are provided to Customer on a secure and regular basis.

### 14.3. Open-source software management

The management of open-source software embedded in our software is directly monitored by each product or service line, following the internal SBS guidelines that defines the rules governing the use of certain open-source licenses, the management of vulnerabilities, obsolescence and debt detected by our SBOM control tools (for compatible applications).

### 14.4. Delivery security

A security check applicable to all deliveries of major versions of products is carried out to avoid critical and high breaches.

For delivery: (i) An anti-virus check is carried out on the deliverables; (ii) product updates and releases are delivered in a secure manner by ensuring code integrity; (iii) a mechanism is in place to allow the Customer to check the origin of the deliverable and verify that it has not been altered (authenticity); If necessary, a hash-code is communicated to the customer in a secure manner.

## 15. Supplier relationship

Security in the relationship with suppliers is overseen by SBS's PSI.

## 16. Compliance

### 16.1. Objectives

To avoid any violation of legal, regulatory or contractual obligations and security requirements.
Ensure compliance of systems with SBS and 74Software security policies and standards.

### 16.2. Measures

The measures in place must prove their effectiveness. Security performance is measured by the formalization of objectives and associated indicators that are reported by the SBS CISO to the General Management.
The monitoring in place to comply with SBS requirements is as follows:

- Follow-up by the monthly security committee dedicated to the product or service line
- Follow-up in IAM risk committees
- Monitoring via SBS's annual information security control plan. Indicators include monitoring of vulnerabilities, business continuity, audits, training; these indicators are evaluated monthly and reviewed annually.
- Regular monitoring of the product or service line for any security alerts or events.

In the event that the Agreement between SBS and the Customer includes the latter's right to audit, and subject to the signing of a specific confidentiality agreement or an Audit Agreement, the various documents may be presented to the auditors.

### 16.3. Security management and security performance indicators

Security indicators are established and monitored by the ISO of the product or service line. KPIs are periodically reported to SBS's CISO.

### 16.4. Continuous improvement

Regular feedback from compliance teams, auditors, and employees are collected and analyzed to continuously improve security measures and compliance efforts.

## 17. Reference documents

- SBS's Information Security Policy, including SBS's Security Incident Management Policy
- The “Common Security Development Guide”
- Charter for the use of computer equipment
- Annual internal memorandum on the Information Security organization
- DSIS of the sites.

## 18. Abbreviations and acronyms

| Abbreviation | Definition |
|---|---|
| AD | Active Directory |
| BU | Business Unit |
| CERT | Computer Emergency Response Team |
| CISO | Chief Information Security Officer |
| Customer | The customer who subscribed for the provisioning of the Solution as stipulated in the Agreement |
| DPO | Data Protection Officer |
| EDR | Endpoint Detection and Response |
| IT Dep | Information Technology Department |
| ISO | Information Security Officer |
| ISP | Information Security Policy |
| IAM | Internal Approbation Meeting. An Iteration Assessment Report (IAR) is presented during this meeting |
| KPI | Key Performance Indicator |
| OWASP | Open Web Application Security Project |
| RGPD | Règlement Général de Protection des Données |
| SISD/ DSIS | Site Infrastructure Security Document File, is a document describing physical security of the premises.In French Dossier de sécurité infrastructure site |
| SBS | SBS Software a subsidiary of 74 Software Group (hereafter “the Group”) |
| SBOM | Software Bill Of Material |
| SMP | Security Management Plan |
| Vulnerability | A weakness of an asset or group of assets that can be exploited by one or more threats |