SBS

Plan d’Assurance Sécurité

Edition, Maintenance et Support

Version 2025.1

Statut : Validé 23/05/2025

1. Présentation du Plan d'Assurance Sécurité

Ce Plan d'Assurance Sécurité (« PAS ») décrit les mesures de sécurité, l'organisation et les processus mis en place par SBS dans le cadre de ses activités d'édition de progiciels, incluant la fourniture de support et de maintenance à ses clients. Tous les termes en majuscules non définis dans ce PAS auront la signification qui leur est donnée dans d'autres parties du Contrat.

Le document décrit les dispositions relatives à la disponibilité, l'authenticité, l'intégrité et la confidentialité concernant la protection des informations, y compris les Données Personnelles.

2. Clause de réversibilité

SBS assure la conformité avec le PAS et les niveaux de sécurité pendant la durée du Contrat et la phase de réversibilité. Tout transfert de données nécessite une validation préalable de l'ISO de SBS et du contact sécurité du Client.

3. Audit de sécurité

SBS réalise des audits de sécurité réguliers, adaptés à chaque ligne de produit ou de service et à la portée spécifique. Ces audits peuvent inclure des évaluations techniques, des évaluations externes et des tests de pénétration. Le Client peut réaliser des audits à ses propres frais, conformément aux conditions définies dans les Conditions Générales (CG) et les Conditions Particulières (CP).

4. Clause de sécurité de la sous-traitance

SBS est responsable des procédures de sécurité de ses sous-traitants.

5. Organisation de la sécurité

5.1. Politique de sécurité de l'information

La Politique de sécurité de l'information (PSI) de SBS est gérée par le CISO de SBS.
La PSI de SBS sont disponibles pour tous les employés via l'intranet.
La PSI peut être présentée lors des audits réalisés par le Client.

5.2. Comité de sécurité

SBS a mis en place un comité de sécurité interne qui se réunit régulièrement au sein des lignes de produit et de service. L'objectif du comité de sécurité interne est de contrôler l'application du PAS en présentant des indicateurs clés de sécurité et des informations clés.
En fonction des options/services souscrits par le Client, un comité de sécurité client se réunira à des périodes régulières.

5.3. Organisation du Client

Le Client a l'obligation de nommer un contact de sécurité chargé d'appliquer la politique de sécurité de l'information du Client. Il sera le point de contact privilégié pour SBS sur les questions de sécurité et le point de contact pour les audits de sécurité, l'envoi de la documentation de sécurité, les comités de sécurité ou d'autres sujets de sécurité. En cas d'incident ou de menace de sécurité, il sera la personne de contact pour les divers échanges et suivis. Les coordonnées du contact de sécurité du Client et du Délégué à la Protection des Données doivent être partagées avec SBS.

5.4. Organisation du département de sécurité de SBS

Objectif. L'objectif est de définir une gouvernance pour la mise en œuvre et la vérification de la Politique de sécurité de l'information de SBS (PSI).

CISO de SBS. Le CISO de SBS est nommé par la direction de SBS.

Officier de la Sécurité de l'Information de la ligne de produit ou de service. L'Officier de la Sécurité de l'Information (« ISO ») affecté spécifiquement à la ligne de produit ou de service de support est responsable de la sécurité dans le cadre du contrat. Les rôles de CISO et ISO sont définis dans des fiches de fonction dédiées validées par la note d'organisation de la sécurité annuelle émise par le CISO de SBS.

5.5. Mission du département de sécurité

L'organisation du département de sécurité est revue annuellement par le CISO de SBS. Le résultat de cette revue est publié en interne pour informer les différentes parties prenantes des rôles, de la mission et des objectifs de sécurité à atteindre pour l'année en cours. La mission du département de sécurité est de :

- Assurer l'application opérationnelle de la Politique de sécurité de l'information (PSI de SBS) et de signaler tout écart (dans son application ou son inadéquation aux activités de SBS)
- Gérer les risques de sécurité et initier des actions pour prévenir les crises et rendre SBS plus résilient en cas de crise
- Aider à mettre en place les moyens nécessaires au niveau de chaque Business Unit (BU) pour atteindre les objectifs de sécurité annuels de SBS
- Sensibiliser les employés aux enjeux de sécurité
- Formaliser et déployer le plan de contrôle de sécurité annuel et soutenir les actions identifiées à la suite de la revue
- Suivre la couverture des vulnérabilités dans les produits SBS et les plans de remédiation associés
- Participer activement aux communautés de sécurité
- Signaler tous les incidents et problèmes de sécurité
- Effectuer une veille de sécurité nécessaire à l'amélioration des processus de sécurité de SBS

Tous les rôles et fonctions de sécurité doivent être validés par le CISO de SBS.

5.6. Gestion des risques

La gestion des risques fait partie intégrante de la gouvernance de la sécurité de SBS. Elle est réalisée de manière continue entre les équipes opérationnelles et l'ISO. SBS a mis en place un processus d'exception de sécurité des risques qui gère les écarts par rapport aux politiques de sécurité établies ou aux exigences spécifiques des lignes de produit et de service.

6. Sécurité des Ressources Humaines

6.1. Objectifs

- S'assurer que les employés de SBS sont conscients de leurs responsabilités et sont aptes aux fonctions qui leur sont assignées conformément aux réglementations en vigueur.
- Réduire le risque de vol, de fraude ou de mauvaise utilisation de l'équipement informatique.
- S'assurer que les employés de SBS sont conscients des menaces à la sécurité de l'information, aux données personnelles ou financières ou à d'autres données confidentielles du Client.
- Réduire le risque d'erreur humaine ou de comportement malveillant en appliquant le principe des « quatre yeux ».
- Vérifier que les comptes et les droits d'accès des employés quittant l'entreprise sont effectivement désactivés. Lorsqu'un employé quitte l'entreprise, tous les droits sont révoqués automatiquement.
- S'assurer que les droits d'accès sont revus régulièrement.

6.2. Sensibilisation et formation à la sécurité

Tous les employés sont régulièrement formés et sensibilisés à la sécurité dans leur contexte. Ils appliquent la « politique de bureau propre ».
Un programme de sensibilisation à la sécurité de l'information définit les exigences de sécurité. La direction est le sponsor de la mise en œuvre de ce programme.
Les collaborateurs accédant aux données de SBS ou de ses clients sont particulièrement sensibles à : (i) la confidentialité des données traitées, (ii) l'éthique de l'entreprise à laquelle le service se rapporte, (iii) l'ingénierie sociale, et (iv) les dommages à l'image et à la réputation de SBS ou de ses clients.

6.3. Mesure de sécurité

Recrutement. Lors du recrutement, le département des ressources humaines effectue des contrôles en fonction de la législation et des règles du pays du futur employé(e).

Clause de confidentialité. SBS s'engage à ce qu'une clause de confidentialité soit systématiquement incluse dans le contrat de travail de ses employés. Les informations couvertes par la clause de confidentialité et l'interdiction de divulgation concernent principalement : (i) le contenu hébergé : les informations ou fonctions traitées par le système, (ii) les informations dont la divulgation pourrait compromettre la sécurité du système (mots de passe, clés de chiffrement, documentation sur l'architecture et la sécurité du système, etc.), (iii) les informations personnelles ou confidentielles du Client, (iv) l'exposition du nom du Client dans des espaces non restreints, (v) en fonction de la portée des services, des clauses supplémentaires peuvent être mises en œuvre.

Formation et sensibilisation. SBS s'engage à ce que ses employés reçoivent une sensibilisation appropriée et des mises à jour régulières sur les exigences de sécurité liées aux réglementations des services fournis, aux mesures de contrôle et plus spécifiquement à la gestion des données. Pour les employés de SBS, SBS met en œuvre le programme de formation à la sécurité de SBS. Par l'intermédiaire de son université de formation, il assure un niveau de sensibilisation à la sécurité de base pour tous ses employés. Les formations traitent des sujets suivants : (i) Bases de la sécurité pour tous, (ii) Sécurité dans les développements (formation dispensée en fonction du rôle/fonction de l'employé), (iii) Protection des données, (iv) Campagne annuelle de test de prévention du phishing.

Résiliation ou modification du contrat de travail. Tout employé de SBS ou sous-traitant qui cesse de travailler voit tous ses droits d'accès retirés. Les accès spécifiques des administrateurs éventuels sont également coupés.

7. Sécurité des actifs

7.1. Objectif

Définir, mettre en œuvre et maintenir des mesures techniques appropriées pour protéger les actifs du système d'information contre les menaces provenant des risques identifiés.

7.2. Exigences de SBS

Les différentes configurations des postes de travail, qui, en fonction du service, se connectent au système d'information ou aux plateformes de développement, sont décrites et qualifiées.
Les règles de classification de l'information (comptes rendus, documents, documents de référence, bases de données, fichiers de données, courriels, etc.) de SBS ou des clients sont identifiées et appliquées (voir chapitre Classification de l'information).
Tous les équipements qui composent le système d'information, les postes de travail de SBS et l'infrastructure pour la fourniture des Services disposent d'un logiciel de protection antivirus à jour.
La mise à jour (récupération et distribution) des bases de signatures et des logiciels antivirus est effectuée sur les postes de travail et les serveurs au moment de la publication par les éditeurs.

7.3. Mesure de sécurité du lieu travail du collaborateur

7.3.1. Ordinateurs portables

Les postes de travail utilisés par les équipes de SBS sont fournis par la DSI et sont donc conformes à la politique de gestion des correctifs en termes de couverture « antivirus » et d'application des correctifs de sécurité Windows.
Le « master » des postes de travail est assurée par la DSI, ainsi que les processus de fourniture, de recyclage et de destruction des postes de travail.
Les postes de travail sont toujours dans une version maintenue de Microsoft Windows et disposent par défaut d'un outil de chiffrement de disque dur.
Chaque employé doit verrouiller son écran lorsqu'il quitte son poste de travail ou le laisse sans surveillance. Par défaut, l'écran se verrouille après quelques minutes d'inactivité pour éviter le vol ou la perte de données.

L'utilisation de ressources non standard (BYOD) n'est pas autorisée pour accéder aux environnements de production de nos clients.

7.3.2. Microsoft Office 365

Les outils collaboratifs et de messagerie utilisés sont fournis à partir de la version cloud de Microsoft, gérée par la DSI. Le système de messagerie dispose d'une solution de sécurité antivirus et anti-spam, ce qui limite le risque de propagation d'un virus.
Les échanges avec les clients par courriel doivent respecter les règles de classification de l'information de SBS et les règles d'utilisation du Client.
SBS permet à ses employés d'avoir un accès courriel sur leur téléphone professionnel ou personnel.
Dans tous les cas, le chiffrement de la base de données Outlook est automatique. Il est contrôlé par un processus MDM (Mobile Device Management).
Par défaut, les passerelles de messagerie de SBS utilisent le protocole TLS 1.2, ce qui permet le chiffrement des messages envoyés. Si la passerelle du Client n'accepte pas le niveau de chiffrement de SBS, aucun message ne sera envoyé jusqu'à ce qu'une méthode sécurisée ait été convenue.

7.3.3. Mobilité

Les employés télétravaillent selon les dispositions mises en œuvre par SBS. Dans ce cas, ils doivent respecter les directives de SBS et suivre les différentes règles de sécurité définies dans les directives.
Un contrôle de conformité est effectué pour vérifier la conformité du poste de travail de l'employé (exemple : antivirus installé et à jour, mises à jour Windows installées, ...) avant de lancer la connexion VPN au réseau SBS.

7.3.4. Médias externes

SBS assure la confidentialité des supports physiques externes nécessaires aux services demandés par le Client : supports papier, si nécessaire.

7.3.5. Base de données des actifs d'exploitations

SBS s'engage à assurer que tous les actifs informatiques ou autres (documents, divers matériels) essentiels à son activité et à la fourniture des services sont protégés conformément aux règles de la Politique de sécurité de l'information. Les actifs sont inventoriés et gérés par produit de manière adaptée au contexte, et le suivi de la sécurité de ces actifs (obsolescence, par exemple) est assuré par l'ISO pour le produit.

7.4. Classification de l'information

Les niveaux de classification sont les suivants :

C1 Public : Un enregistrement contenant des informations non sensibles et non confidentielles est considéré comme non classifié ou public.
C2 Usage restreint (Limité au besoin de savoir) : classification par défaut pour tous les nouveaux documents.
C3 Confidentiel : La divulgation à un tiers interne ou externe non autorisé peut causer un préjudice à SBS, aux clients et aux partenaires ou aux employés.
C4 Strictement confidentiel : La divulgation peut causer un préjudice grave à SBS et à ses clients.

7.5. Protection liée à la manipulation de l'information

Les employés de SBS appliquent plusieurs règles internes mentionnées ci-dessous :

- Dans le contrat de travail pour le respect des exigences légales et réglementaires (RGPD, Accord de travail, politiques internes, charte informatique, etc.),
- Dans les guides et instructions de la DSI pour la sécurité du réseau et des équipements,
- Dans le document de politique de « Classification de l'information » de SBS, qui décrit les différents cas d'utilisation
- Pour les actifs gérés par la DSI, l'intégrité des données dans les journaux d'accès aux systèmes d'information est sous la responsabilité des administrateurs de la DSI.

Destruction de l'information :

Lorsque l'information n'est plus nécessaire, des moyens sont mis à disposition des employés de SBS pour la détruire, par exemple :

- Déchiqueteuse pour les documents papier,
- Procédure déployée par la DSI pour le décommissionnement, la mise au rebut et la destruction des équipements.

8. Protection logique

8.1. Exigences de sécurité

- Toutes les connexions au Système d'Information (SI) de SBS sur lequel SBS fournit les Services à ses clients sont soumises à des procédures (activités de support éditeur, sous-traitants tiers),
- Toutes les connexions effectuées par les administrateurs de l'infrastructure (IM) au Système d'Information (SI) de SBS sur lequel SBS fournit les Services à ses clients sont suivies, protégées et archivées de manière intégrée sur une période glissante,
- En cas de fuite de données ou d'incident, les traces générées peuvent être examinées pour détecter les parties impliquées et les ressources utilisées,
- Les droits d'accès logiques sont soumis à une procédure de contrôle : tout changement de statut (arrivée, départ, changement, etc.) doit être pris en compte. Les droits d'accès doivent être modifiés en conséquence,
- Les utilisateurs doivent être rattachés à un profil lié à leur fonction,
- Les utilisateurs sont automatiquement contraints de changer leurs mots de passe au moins tous les 90 jours, y compris les utilisateurs privilégiés.

8.2. Gestion des comptes utilisateurs internes

8.2.1. Règles concernant les comptes utilisateurs internes

Pour tous les accès aux services, outils ou applications de SBS, les employés de SBS suivent le processus de gestion des demandes de SBS (application de gestion des demandes ITSM).
Les règles suivantes de SBS sont appliquées :

- Un employé de SBS a un identifiant unique et personnel,
- Il est authentifié avec l'Active Directory. Son accès aux différents systèmes dépend directement des droits contenus dans celui-ci,
- Au départ, l'employé dispose au moins d'un compte MS Office, d'un accès Internet, d'une boîte aux lettres, protégée par mot de passe,
- Il a accès uniquement aux applications nécessaires à l'accomplissement de ses missions,
- Certains employés ont des privilèges pour effectuer l'administration, la maintenance ou les mises à jour des systèmes et applications ; leur nombre est réduit au minimum et les privilèges sont revus régulièrement ; ces utilisateurs utilisent une authentification forte,
- Une politique de gestion des mots de passe est définie et appliquée,
- Les mots de passe respectent la politique de mots de passe de SBS,
- La politique sécurité interdit à l'employé de divulguer ses informations d'authentification,
- Les droits d'accès des employés ne sont pas transférables,
- L'accès au système est ralenti puis bloqué après un certain nombre de tentatives d'authentification échouées, comme défini dans la PSI,
- Lorsqu'un employé quitte l'entreprise, il perd automatiquement tous ses droits d'accès
- Les utilisateurs sont déconnectés après une certaine période d'inactivité,
- Éviter les comptes génériques. Si l'utilisation de comptes génériques ne peut être évitée, les fichiers de trace permettent de consigner les activités effectuées par les utilisateurs au moyen de ces comptes génériques,
- Changer systématiquement les comptes fournis par défaut par les fabricants et éditeurs,
- Générer et stocker les mots de passe de manière sécurisée

8.2.2. Gestion des droits d'accès pour les utilisateurs internes

Attribution / modification des droits d'accès :

- Les demandes de création ou de modification des droits d'accès à des applications et services spécifiques sont soumises à validation par le responsable hiérarchique (ou le responsable de l'application)
- Les droits d'accès logiques sont accordés en fonction des besoins de l'employé et de sa fonction. L'octroi de ces droits est systématiquement suivi.

8.2.3. Retrait des droits d'accès pour les personnes en fin de contrat

Dès qu'un employé quitte l'entreprise, les procédures internes de l'entreprise sont appliquées et tous les droits d'accès aux applications de l'entreprise sont supprimés. Le processus de départ par défaut est lancé le jour suivant.

8.2.4. Revue des droits d'accès

Les revues d'accès sont déterminées en fonction des rôles (administrateurs, utilisateurs, etc.).

8.3. Gestion des comptes sur environnement du Client

8.3.1. Gestion des droits d'accès sur les environnements clients pour les services de support

Pour les activités de Support, la gestion des droits d'accès d'un employé SBS à un environnement Client suivent les procédures du Client et sont sous la responsabilité de ce dernier.

8.4. Outil de ticketing

8.4.1. Autorisations

L'outil de ticketing dispose d'un système de gestion des autorisations qui permet à chaque utilisateur de se voir attribuer un profil. Ce profil définira les actions pouvant être effectuées sur l'outil (consultation de la documentation, consultation des tickets, création de tickets, administration, etc.).

8.4.2. Authentification et mot de passe

L'authentification pour les utilisateurs de SBS est basée sur les règles de l'Active Directory. Les modalités d'accès peuvent évoluer en fonction des besoins exprimés par SBS.

8.4.3. Attribution / modification des droits d'accès

Lorsqu'un employé doit utiliser l'outil de ticketing, un compte est créé et un profil lui est attribué en fonction de ses besoins. Une revue des droits d'accès est effectuée régulièrement.

8.4.4. Retrait des droits d'accès pour les personnes en fin de contrat

Pour les utilisateurs de SBS, le verrouillage du compte de l'AD bloquera l'accès à l'outil de ticketing.
Il appartient au point de contact du Client de gérer les entrées/sorties des utilisateurs du Client et faire les demandes nécessaires à SBS.

9. Sécurité physique

9.1. Sécurité physique dans les locaux de SBS

L'organisation en charge de la gestion des locaux veille à ce que les services requis en termes de services généraux (électricité, climatisation, etc.), de sécurité incendie et de services anti-intrusion soient conformes aux normes et exigences de sécurité imposées par les réglementations locales, les compagnies d'assurance et la PSI:

- Par défaut, les collaborateurs de chaque site utilisent un système de contrôle d'accès par badge centralisé. Ce système est utilisé pour restreindre l'accès aux locaux aux seules personnes autorisées,
- Si nécessaire, les locaux sont divisés en zones pour contrôler l'accès,
- Les salles informatiques (ou salles techniques) ont un accès restreint,
- En fonction du pays, le règlement intérieur du site décrit les consignes de sécurité sur les sites et est accessible à tous les employés du site (via affichage sur site),
- Les systèmes électriques d'urgence et de climatisation sont dimensionnés en fonction du site et de sa criticité,
- Le site peut avoir une surveillance à distance pour le site (par exemple, les portes d'accès aux locaux, les fenêtres au rez-de-chaussée, les portes des salles machines, etc.),
- La gestion de l'accès physique est de la responsabilité du Gestionnaire de site du bailleur et du Secrétariat Général de SBS ou de son équivalent dans d'autres pays,
- La responsabilité des personnes et des biens est confiée au Directeur de site qui est soutenu par le responsable de site du bailleur,
- Le Document de Sécurité de l'Infrastructure du Site (« DSIS ») résume ces exigences pour chacun des sites.

9.1.1. Objectif

- Prévenir l'accès physique non autorisé, les dommages ou les intrusions dans les locaux.
- Prévenir la perte, les dommages, le vol ou la compromission des biens et la perturbation des opérations de SBS.

9.1.2. Document de Sécurité de l'Infrastructure du Site (« DSIS ») des sites

Les sites de SBS sont gérés par 74Software, ou par SBS en direct ou par le bailleur de SBS (SSG).

Un responsable de site est affecté à chaque site, son rôle est de mettre en œuvre les mesures de sécurité du site conformément à la Politique de Sécurité de l'Information.
Un DSIS (document de sécurité de l'infrastructure du site) est présent sur chaque site, sous la responsabilité des responsables de site et des services généraux.
Les actions identifiées dans le DSIS et les exigences prises par le service incluent :

- La prévention des accès physiques non autorisé, les dommages ou les intrusions dans les locaux du Service et les informations,
- La prévention de la perte, les dommages, le vol ou la compromission des biens et la perturbation des opérations du Service

10. Gestion des incidents de sécurité

10.1. Objectif

S'assurer que les procédures de signalement des incidents de sécurité de l'information permettent une action corrective rapide.
Mettre en œuvre une politique et des processus cohérents et efficaces pour la gestion des incidents de sécurité de l'information.
S'assurer que le signalement rapide de tous les événements de sécurité de l'information par les canaux de signalement appropriés est en place.

10.2. Événement de sécurité

Un événement de sécurité est un événement qui attire l'attention en raison de son potentiel à compromettre la sécurité du système ou des données.

10.3. Incident de sécurité

Après analyse, un événement peut être requalifié en incident de sécurité lorsque l'intégrité, la confidentialité ou la disponibilité de l'information est potentiellement compromise de manière indésirable ou non autorisée. Un incident de sécurité peut nécessiter des actions correctives, une gestion de crise, le signalement de l'incident et l'évaluation post-incident.

10.4. Procédures

SBS applique la politique de gestion des incidents de sécurité définie dans sa PSI. Cette dernière spécifie le processus d'escalade, les personnes à contacter et à tenir informées, et la formation de la cellule de crise qui sera activée en cas d'incident de sécurité majeur. Compte tenu de la nature des informations contenues dans cette procédure, ce document est confidentiel.
Le processus de gestion des incidents de sécurité implique trois niveaux :

- Le niveau local, dès que l'incident est détecté au niveau opérationnel,
- Le niveau entité et site, après escalade,
- Le niveau SBS puis 74Software après escalade.

Le processus de suivi d'un incident est le suivant : Signalement, Collecte de preuves ; Analyse, Escalade possible, Traitement, Communication, Analyse post-incident.

10.5. Déclaration et suivi

L'ISO de la ligne de produit ou de service de Support est informé par les équipes de la ligne de chaque incident de sécurité. Dans le cadre du Support, tous les incidents de sécurité de l'information affectant SBS et les services souscrits par le Client doivent être notifiés au Client dans les délais réglementaires (maximum 24 heures) suivant la qualification de ces incidents par l'ISO.
Une procédure existe et elle est partagée sur demande. La procédure contient des informations concernant la notification, les descriptions, les remédiations et les leçons apprises.

Il est possible de déclarer un incident de sécurité via l'outil de ticketing également, si l'incident de sécurité est considéré comme critique par SBS, il sera traité comme un incident critique (P1). Les délais de traitement des incidents sont indiqués dans le Contrat. Dans d'autres cas, il sera traité par l'ISO de la ligne de produit ou de service dès que possible.

En cas d'incident de sécurité, SBS appliquera tous les moyens pour collaborer avec le CISO du Client ou à défaut le contact de sécurité désigné, assurant une communication transparente et en participant activement à fournir les preuves nécessaires à l'analyse et à la remédiation de l'incident de sécurité.
Pour contacter SBS, une adresse e-mail spécifique est fournie : security.incident@sbs-software.com

10.6. Incidents impactant les données personnelles (RGPD)

Le processus de gestion des incidents de sécurité inclut la gestion des violations de données personnelles. Les incidents sont signalés au responsable du traitement des données de SBS dès que possible et suivent les exigences réglementaires.
Si l'incident impacte des données personnelles, des informations supplémentaires doivent être communiquées au DPO de 74Software et du Client s'il est impacté.
L'adresse e-mail du DPO de 74Software est GDPR.ACCESS@sbs-software.com

10.7. Signalement

Tous les employés et sous-traitants doivent signaler ces problèmes à leur responsable dès que possible pour éviter les incidents de sécurité de l'information. Le signalement des incidents de sécurité se fait via l'application de gestion des services informatiques ITSM, qui dispose d'un processus dédié aux incidents de sécurité.

11. Gestion de la continuité des activités

SBS dispose des moyens organisationnels et techniques pour assurer la continuité de ses activités d'Edition et des Services fournis à ses Clients.
SBS s'efforce de maintenir le niveau de service défini dans le Contrat de chaque Client, de protéger les processus métier critiques des effets d'une défaillance du système d'information, et d'assurer la reprise de ces processus dès que possible. En cas d'incident affectant la disponibilité du service, SBS s'engage à restaurer le Service tel que défini dans le Contrat.
SBS maintient des documents décrivant les mesures de continuité d'activité et un test est réalisé annuellement avec un rapport fourni au client sur simple demande.

12. Chiffrement

12.1. Objectif

Assurer l'utilisation correcte du chiffrement pour protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

12.2. Exigences

Une politique d'utilisation des mesures cryptographiques pour protéger l'information a été développée et mise en œuvre par SBS.

12.3. Chiffrement au repos

Ordinateur portable de l'entreprise
Tous les postes de travail de SBS sont chiffrés au repos (la Solution déployée par la DSI est actuellement Bitlocker). SBS s'engage à utiliser des protocoles de chiffrement robustes sans vulnérabilités connues.

12.4. Chiffrement des données en transit

Par défaut, un protocole de transfert chiffré (sFTP, HTTPS, ...) doit être mis en œuvre pour les échanges de données entre SBS et les clients.
Pour les flux de communication chiffrés, le protocole TLS 1.2 est appliqué, ou une version TLS supérieure dès que celle-ci est validée par SBS.
Cette mesure est obligatoire lorsque des Données Clients sont présentes dans l'environnement.
Une mesure compensatoire peut-être la mise en place d'un VPN si le flux est en clair.

13. Sécurité des opérations de service

13.1. Sauvegarde

Dans le cadre de l'activité de Support, SBS s'engage à sauvegarder l'infrastructure nécessaire au fonctionnement du service avec le Client. SBS est responsable de la restauration, en utilisant la dernière sauvegarde effectuée, de toutes les données, fichiers ou informations perdus ou endommagés.

13.2. Séparation des environnements

La R&D de SBS dispose de ses propres environnements de développement dédiés à chaque activité : tests, qualification, intégration, …

Dans le cadre de l'activité de Support, et sauf demande explicite d'un Client, des données de production ne sont pas copiées dans des environnements de SBS.

13.3. Protection contre les logiciels malveillants

Les antivirus et EDR sont déployés sur tous les postes de travail des employés de SBS. Les antivirus et EDR sont déployés au minimum sur tous les systèmes d'exploitation Windows, et sur certains environnements Linux.
La surveillance des antivirus est effectuée par la DSI. Un reporting mensuel du niveau de sécurité du parc informatique est présentée au comité de sécurité de SBS.

13.4. Journalisation et suivi

13.4.1. Synchronisation d'horloge

Pour les systèmes de journalisation, une horloge maîtresse permet de garantir que tous les serveurs sont synchronisés sur la même base temps.

13.5. Gestion des vulnérabilités sur les infrastructures de développement

13.5.1. Criticité et notation CVSS

La gestion des vulnérabilités est analysée et rapportée, avec une évaluation basée sur la notation CVSS 3 brute :

L'impact des vulnérabilités peut varier, il peut être recalculé automatiquement ou manuellement en fonction de certains paramètres tels que l'exposition de l'actif concerné, son environnement, ... Les vulnérabilités considérées comme Critiques (CVSS contextualisé ≥9) et prouvées sont considérées comme un incident P1 et traitées immédiatement.

13.5.2. Surveillance des vulnérabilités

Le service de surveillance des vulnérabilités est organisé chez SBS et repose principalement sur :

- Les bulletins CERT de l'unité de cybersécurité du groupe Sopra Steria
- Un abonnement à un CERT privé

La gestion des correctifs de sécurité appliqués aux postes de travail et aux serveurs est effectuée par la DSI et un rapport mensuel sur les postes de travail est mis à disposition du CISO. Pour les serveurs gérés par les équipes opérationnelles, la même obligation de gestion des correctifs est portée.
En cas de déviation, une exception de sécurité est gérée par les équipes sécurité.

13.6. Connexions aux environnements du Client

Connexion depuis SBS
Exceptionnellement dans le cadre de ses activités de Support, SBS peut être amené à se connecter à un environnement Client. Dans ce cas, la connexion est sécurisée, supervisée par le Client, temporaire, limitée en nombre de collaborateurs SBS et restreinte aux actions strictement nécessaires.

14. Sécurité dans le développement

14.1. Développement de logiciel

14.1.1. Sécurité dans le développement

SBS a créé pour ses besoins une politique d'obsolescence des logiciels ainsi qu'un guide de développement sécurisé**.** Ce document fournit un guide de codage non-agnostique pour protéger les produits de SBS des menaces listées dans le référentiel OWASP[1] Top 10. Ce document est applicable à tous les produits de SBS et il est enrichi par des documents complémentaires.

La gestion de l'obsolescence des composants et produits tiers, la gestion des licences des logiciels open-source et la gestion des vulnérabilités sont traités dans des chapitres spécifiques plus bas.

14.1.2. Audits et revues de sécurité

Pendant le développement et au cours de la vie d'un produit de SBS, des audits et revues de sécurité sont réalisés :

- De façon statique par analyse du code source (revue « 4-yeux », Static Application Security Testing - SAST, Software Composition Analysis - SCA, Software Bill of Materials – SBOM) ou de façon dynamique à travers les Application Security Audit - ASA, et les tests d'intrusion
- Pour vérifier que les règles de sécurité ont bien été respectées pendant le cycle de développement,
- Pour identifier toutes les vulnérabilités qui pourraient conduire à l'exploitation de failles de sécurité et identifier les actions de remédiation pour ces dernières.

La surveillance des vulnérabilités à travers le suivi des bulletins CERT est également intégrée dans le développement et le cycle de vie des logiciels (cf *supra*).

14.1.3. Analyse automatique et déploiement

Quand cela est possible, des outils de Software Composition Analysis (SCA) et de Static Application Security Testing (SAST) sont intégrés dans le processus d'intégration continue du produit de façon à vérifier que les nouveaux développements n'intègrent pas de nouvelles vulnérabilités.

14.1.4. Gestion des vulnérabilités

Chaque vulnérabilité est affectée d'un niveau de criticité et d'un niveau de priorité
Le traitement des vulnérabilités suit le processus de correction défini ci-dessous.

Score CVSS brut des vulnérabilités

La criticité est calculée en utilisant la notation CVSS brut déjà présentée précédemment. La détermination de la criticité tient compte de tous les critères incluant la complexité de l'attaque, l'exploitation et l'existence d'une remédiation à la vulnérabilité.
Si pour une raison quelconque, la notation CVSS n'est pas adaptée, un autre référentiel validé par la communauté des ISO de SBS peut être employé.

Criticité et priorité après contextualisation

Une vulnérabilité est contextualisée exclusivement par SBS, en termes d'impact métier, de probabilité et d'exploitation, pour définir une priorité.

Les processus de correction, d'information aux clients et de livraison sont adaptés à la priorité de la vulnérabilité. La remédiation est prioritairement réalisée sur la version la plus récente puis en conformité avec la politique Editeur sur les versions maintenues.

Suivi des vulnérabilités

Les vulnérabilités sont tracées et surveillées par l'ISO de la ligne de produit ou de service.

14.2. Cycle de vie du développement logiciel sécurisé

Conformément aux bonnes pratiques, toutes les versions de logiciel sont identifiées de manière unique et suivies tout au long de leur cycle de vie ; tous les changements sont clairement associés à une version de logiciel unique.

La gestion des changements au cours du cycle de vie du logiciel permet que tous ceux-ci soient identifiés, évalués et approuvés. Un processus est en place, permettant l'enregistrement des demandes, leur justification, l'analyse de leur impact et la décision finale. Cela inclut l'approbation par le personnel responsable, la traçabilité des personnes ayant créé/modifié le code source et l'exécution éventuelle de tests de sécurité complémentaires avant livraison.

La protection de l'intégrité du logiciel tout au long de son cycle de vie est l'objet d'un processus mature. Des mécanismes et des outils sont en place pour protéger l'intégrité du code source et des composants tiers embarqués ; ils permettent d'identifier toutes les modifications et les personnes concernées par celles-ci.

Les menaces et les vulnérabilités dans le design du logiciel sont identifiées et évaluées de façon continue : un processus clair et mature est en place pour enregistrer l'inventaire des menaces et les failles, le résultat des évaluations, les décisions de remédiation ou d'atténuation et les approbations ; il est régulièrement exécuté durant le cycle de vie logiciel.

L'objectif de la détection et de l'atténuation des vulnérabilités est de garantir, par des contrôles réguliers, que les produits développés par SBS ne contiennent aucune vulnérabilité critique ou élevée connue au moment de la livraison au Client. Pour cela, la base code complète est analysée, y compris les composants et librairies tiers, partagés et open-source.
Les parties prenantes sont informées à propos des problèmes de sécurité potentiels et des options d'atténuation.
Les mises à jour de sécurité sont fournies au Client de manière sûre et régulière.

14.3. Gestion des logiciels open-source

La gestion des logiciels open-source intégrés dans nos logiciels est directement surveillée par chaque ligne de produit ou de service, suivant les directives internes de SBS qui définissent les règles régissant l'utilisation de certaines licences open-source, la gestion des vulnérabilités, de l'obsolescence et de la dette détectées par nos outils de contrôle SBOM (pour les applications compatibles).

14.4. Sécurité des livraisons

Un contrôle de sécurité applicable à toutes les livraisons de versions majeures de produit est réalisé pour éviter les failles critiques et hautes.

Pour les livraisons : (i) Un contrôle anti-virus est réalisé sur les éléments livrables ; (ii) les mises à jour et les versions de produit sont délivrées de façon sûre en garantissant l'intégrité du code ; (iii) un mécanisme est en place pour permettre au Client de contrôler l'origine du livrable et vérifier qu'il n'a pas été modifié (authenticité) ; si nécessaire un « hash-code » est communiqué au client de façon sécurisée

15. Relations avec les fournisseurs

La sécurité dans la relation avec les fournisseurs est encadrée par la PSI de SBS.

16. Conformité

16.1. Objectifs

Éviter toute violation des obligations légales, réglementaires ou contractuelles et des exigences de sécurité. Assurer la conformité des systèmes avec les politiques et normes de sécurité de SBS et de 74Software.

16.2. Mesures

Les mesures en place doivent prouver leur efficacité. La performance de la sécurité est mesurée par la formalisation d'objectifs et d'indicateurs associés qui sont rapportés par le CISO de SBS à la Direction Générale. La surveillance en place pour se conformer aux exigences de SBS est la suivante :

- Suivi par le comité de sécurité mensuel dédié à la ligne de produit ou de service
- Suivi dans les comités de risque IAM
- Surveillance via le plan de contrôle annuel de la sécurité de l'information de SBS. Les indicateurs incluent la surveillance des vulnérabilités, de la continuité d'activité, des audits, de la formation, ces indicateurs sont évalués tous les mois et revus annuellement.
- Surveillance régulière de la ligne de produit ou de service pour toute alerte ou événement de sécurité.

Dans le cas où le Contrat entre SBS et le Client inclut le droit d'audit de ce dernier, et sous réserve de la signature d'un engagement de confidentialité spécifique ou d'un Accord d'Audit, les différents documents peuvent être présentés aux auditeurs.

16.3. Gestion de la sécurité et indicateurs de performance de la sécurité

Des indicateurs de sécurité sont établis et surveillés par l'ISO de la ligne de produit ou de service. Les KPI sont périodiquement rapportés au CISO de SBS.

16.4. Amélioration continue

Des retours réguliers des équipes de conformité, des auditeurs et des employés sont collectés et analysés pour améliorer continuellement les mesures de sécurité et les efforts de conformité.

17. Documents de référence

- La Politique de Sécurité de l'Information de SBS, y compris la politique de gestion des incidents de sécurité de SBS
- Le « Common Security Development Guide »
- Charte d'usage des équipements informatiques
- Note interne annuelle sur l'organisation de la Sécurité de l'Information
- DSIS des sites.

18. Abréviations et acronymes

Abréviation	Définition
AD	Active Directory
BU	Business Unit
CERT	Computer Emergency Response Team
Client	Le client qui a souscrit à la fourniture d'un service comme stipulé dans le Contrat
CISO	Chief Information Security Officer, RSSI en français
DPO	Data Protection Officer
DRP	Disaster recovery Plan, Plan de Reprise d'Activité en français
DSI	Direction Système d'Information
DSIS / SISD	Dossier de Sécurité Infrastructure Site
EDR	Endpoint Detection and Response
IAM	Internal Assessment Meeting

ISO	Information Security Officer
KPI	Key Performance Indicator
OWASP	Open Web Application Security Project
PAS	Plan d'Assurance Sécurité
PSI	Politique de Sécurité de l'Information
RGPD	Règlement Général de Protection des Données
SBOM	Software Bill Of Material
SBS	SBS Software, une filiale de 74 Software Group
SMT / ITSM	Outil de gestion des services de support SBS, permettant la gestion des incidents, des changements, des problèmes, des versions. Cet outil est utilisé pour capturer et suivre les incidents et les demandes.
Vulnérabilité	Une faiblesse d'un actif ou d'un groupe d'actifs qui peut être exploitée par une ou plusieurs menaces