
SBS

Plan d'Assurance Sécurité
Services Managés SAB

Version 2025.3 – 01/10/2025

Statut : Approved

1. Présentation du Plan d'Assurance Sécurité

Ce Plan d'Assurance Sécurité (« PAS ») fait partie intégrante du Contrat conclu entre le Client et SBS et vient le compléter. Il présente les mesures de sécurité, l'organisation et les processus mis en œuvre par SBS dans le cadre de la prestation des Services. Ce PAS s'applique aux environnements de production et non-production (hors bases mortes) du Client opéré sur l'infrastructure des Services Managés SAB. L'infrastructure et les mesures de sécurité sont mises en œuvre progressivement pendant la durée du projet de mises en œuvre des services managés (phase de Build) et sont appliquées dans leur globalité dès la phase de Run. Certains indicateurs de sécurité ou exigences techniques peuvent être ajustés en fonction de leur criticité et de leur exposition. Tous les termes en majuscules ont le sens qui leur est attribué dans les autres parties du Contrat.

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

2. Clause de réversibilité

SBS veillera à garantir la conformité avec le PAS ainsi qu'aux niveaux de sécurité définis, pendant toute la durée du Contrat y compris la phase de réversibilité. Tout transfert de données doit faire l'objet d'une validation préalable de l'ISO de SBS et du contact sécurité du Client. Les demandes spécifiques liées à la réversibilité font l'objet d'une proposition commerciale dédiée. SBS maintient par ailleurs des processus de réversibilité documentés.

3. Audit de sécurité

SBS réalise régulièrement des audits de sécurité, adaptés à la nature des services fournis et sur le périmètre mutualisé de la prestation délivrée aux clients de l'offre SAB en services managés. Ces audits peuvent inclure des évaluations techniques, des audits externes et des tests de d'intrusion.

Le Client peut effectuer ses propres audits, à ses propres frais, conformément aux modalités prévues dans les Conditions Générales (CG) et les Conditions Particulières (CP).

4. Clause de sécurité globale

SBS est responsable de la mise en œuvre et du suivi des procédures de sécurité et de ses sous-traitants. Des contrôles réguliers sont effectués afin de vérifier la conformité aux exigences de sécurité et de ces sous-traitants. (Un contrôle a minima est réalisé chaque année, conformément aux exigences de certification en vigueur).

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 est disponible 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. Ce comité a pour mission de superviser l'application du PAS en s'appuyant sur des indicateurs de sécurité clés de sécurité et des informations stratégiques.

Selon les options ou services souscrits par le Client, un comité de sécurité dédié pourra être organisé à intervalles réguliers.

5.3. Organisation du Client

Le Client est tenu de désigner un référent de sécurité veiller à l'application de 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 ou d'autres sujets de sécurité et les comités de sécurité. En cas d'incident ou de menace de sécurité, il sera le point de contact pour les divers échanges et suivis. Les coordonnées du référent 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 service. L'Officier de la Sécurité de l'Information (« ISO ») sera spécifiquement désigné pour la ligne de service et spécifiquement au Client. Il ou elle sera désigné(e) dans le PAS en tant que responsable de la sécurité pour le Client sur la ligne nommée ISO de la ligne de service. Les rôles de CISO, ISO et PSL (Project Security Leader) 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 diffusé en interne pour informer les différentes parties prenantes des rôles, mission et objectifs de sécurité fixés pour l'année en cours. La mission du département de sécurité est de :

- Assurer la mise en œuvre 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
- Accompagner les Business Units (BU) dans la mise en place des moyens nécessaires à l'atteinte des objectifs de sécurité définis annuellement.
- Sensibiliser les collaborateurs aux enjeux de sécurité de l'information
- Elaborer et déployer le plan de contrôle de sécurité annuel et suivre la mise en œuvre des actions identifiées issue de la revue annuelle,
- Assurer le suivi des vulnérabilités au sein de nos produits et les plans de remédiation associés
- Identifier les activités nécessitant une certification (en particulier ISO/IEC 27001), et accompagner les projets de certification ainsi que leur suivi annuel
- Participer activement aux communautés de sécurité
- Signaler tous les incidents et problèmes de sécurité.
- Contribuer aux « communautés de sécurité externes » et assurer une veille continue pour améliorer les dispositifs et processus de sécurité de SBS
- L'ensemble des rôles et fonctions de sécurité doivent être validés par le CISO de SBS.

5.6. Gestion des risques

SBS applique la méthodologie de gestion des risques définie par SBS. Cette méthodologie est basée sur les principes de l'ISO/IEC 27005 et de l'EBIOS (ANSSI). Cette analyse des risques est révisée chaque année. Les critères d'évaluation des risques de sécurité au sein de la ligne de service sont définis par l'ISO. Leur principal objectif est de déterminer les niveaux de risque acceptables. Les risques résiduels identifiés sont présentés à la direction de la ligne de service pour validation et acceptation.

L'analyse des risques fait partie intégrante de la gouvernance de la sécurité de SBS. Elle est conduite de manière continue, en collaboration entre les équipes de maintenance opérationnelle et l'ISO. SBS a mis en place un processus d'exception de sécurité des risques (« Security Exception ») qui gère les écarts par rapport aux politiques de sécurité établies ou aux exigences spécifiques des lignes 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 après un maximum de 45 jours.

S'assurer que les droits d'accès sont revus trimestriellement.

6.2. Sensibilisation et formation à la sécurité

Tous les employés (y compris l'équipe d'opérations) sont régulièrement formés et sensibilisés à la sécurité dans leur contexte. Ils appliquent par exemple une « 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 opérateurs 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 (screening) en fonction de la législation et des règles du pays du futur employé(e). Les contrôles suivants sont effectués : (i) contrôle d'identité, (ii) preuve de « diplôme » / certification, (iii) casier judiciaire pour les nouveaux arrivants de l'équipe des opérations.

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 y compris ses équipes d'opérations, 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 département de formation, il assure un niveau de sensibilisation à la sécurité de base pour tous ses employés. Les cours de formation peuvent être complétés par le Responsable de la sécurité de l'information des différentes entités. En particulier, les participants sont informés lors de leur intégration au sein du projet ou via les campagnes de sensibilisation à la sécurité planifiées par SBS. Les formations comprennent les bases de la sécurité, la protection des données et la sensibilisation à la corruption. Une campagne annuelle de tests de prévention contre le phishing est organisée.

Résiliation ou modification du contrat de travail. Tout employé de SBS qui cesse de travailler et qui a (ou pourrait avoir) des droits d'accès à un système verra tous ses droits d'accès retirés. Les modalités de restriction d'accès (notamment Active Directory (« AD »)) sont gérées par le département informatique conformément aux dispositions définies dans la PSI de SBS. Toutes les modifications apportées à l'AD de SBS sont déployées quotidiennement et revues trimestriellement. Les accès spécifiques exercés par les équipes d'opérations (et les administrateurs éventuels) sont également coupés. Lorsqu'un employé ou un sous-traitant quitte l'entreprise, sa date de départ est enregistrée par son assistant de direction. Son compte est automatiquement désactivé lorsque sa date de départ est passée. Dès lors, l'employé perd toutes ses autorisations d'accès. Le compte est définitivement supprimé 45 jours après la date de sortie de l'employé.

Rôles et responsabilités Les procédures appliquées par les équipes d'opérations sont documentées et décrivent les rôles et responsabilités des différents intervenants.

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 à la plateforme, sont décrites.

Les règles de classification de l'information (procès-verbaux, documents, documents de référence, bases de données, fichiers de données, courriels, etc.) de SBS ou de ses clients sont identifiées et appliquées (voir chapitre [Classification de l'information](#)).

Tous les équipements qui composent le système d'information des 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.

La protection End Point Detection & Response (EDR) est activée sur tous les postes de travail et les serveurs informatiques internes.

7.3. Mesure de sécurité du lieu travail

7.3.1. Ordinateurs portables

Les postes de travail utilisés par les équipes de SBS sont fournis par le département informatique 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 le département informatique, 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 et les ports USB sont bloqués.

Chaque employé doit :

- Ne laissez pas de documents confidentiels (plus de C2) sans surveillance Verrouiller les écrans lorsqu'ils quittent un poste de travail sans surveillance. Par défaut, l'écran se verrouille après quelques minutes d'inactivité pour éviter le vol ou la perte de données.

Le département informatique recommande les règles suivantes pour les ordinateurs portables :

- Toujours sécuriser l'ordinateur portable lorsqu'il n'est pas sous une surveillance directe.
- Garder l'ordinateur portable avec l'employé.
- Dans les transports en commun, en particulier dans les trains ou les avions, l'ordinateur portable doit rester sous surveillance directe et constante avec le mode écran confidentiel activé (si disponible).

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 le département informatique. 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.

Parce que 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.

Une autre méthode consiste à transférer le message compressé et chiffré AES 256 avec échange de mot de passe par un autre moyen (soit par téléphone, soit par courriel).

7.3.3. Mobilité

Les employés peuvent télétravailler 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 doit assurer la confidentialité des supports physiques externes nécessaires aux services externalisés et demandés par le Client : supports papier, supports de stockage amovibles. Des règles sont mises en œuvre pour la gestion de ces supports physiques externes.

7.4. Base de données des actifs d'exploitation

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 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.

7.5. Classification de l'information

Par défaut, les règles appliquées en termes de confidentialité de l'information sont celles définies dans la PSI. Cet aspect est régi par la politique de sécurité « Gestion des actifs », chapitre « Classification de l'information ».

Les règles de gestion des documents sont appliquées à l'aide de modèles associés.
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.

7.6. Protection liée à la manipulation de l'information

Les employés de SBS doivent appliquer plusieurs règles internes mentionnées :

- 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 du département informatique pour la sécurité du réseau et des équipements,
- Les règles incluses dans la PSI de 74Software et SBS

Pour les actifs gérés par le département informatique, l'intégrité des données dans les journaux d'accès aux systèmes d'information est sous la responsabilité des administrateurs du département informatique,

Pour les actifs dédiés au présent Contrat, l'intégrité des données dans les journaux d'accès est sous la responsabilité des équipes d'opérations SBS.

Destruction de l'information :

Lorsque des informations échangées entre les Parties dans le cadre de la réalisation des services managés ne sont plus nécessaires à la bonne réalisation des services, des moyens sont mis à disposition des collaborateurs SBS pour les détruire. Cela inclut :

- Broyeur pour le papier
- PV dans le cadre d'une destruction d'une bande contenant des données Clients
- PV dans le cadre d'une destruction complète d'un serveur et de ses disques
- Procédure de gestion de l'obsolescence et d'exception de la DSI pour l'IT Group.

Une protection contre la perte de données (DLP) est en place sur les postes de travail SBS et l'infrastructure de messagerie.

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 d'au moins 6 mois,
- En cas de fuite 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,
- Par défaut, les utilisateurs ne sont pas administrateurs de leur poste de travail.

8.2. Gestion des comptes utilisateurs internes

8.2.1. Règles concernant les comptes utilisateurs internes de SBS

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,
- Il a accès uniquement aux applications nécessaires à l'accomplissement de ses missions,
- 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,
- Certains employés (comptes administrateurs uniquement) ont des privilèges pour effectuer l'administration, la maintenance ou les mises à jour des systèmes et applications. Ces utilisateurs doivent utiliser une authentification forte basée sur une gestion décentralisée des droits sur l'Active Directory d'IMT indépendants de ceux mentionnés ci-dessus,
- Les comptes administrateurs non utilisés sont automatiquement désactivés après 45 jours d'inactivité,
- Une politique de gestion des mots de passe est définie et appliquée,
- Lorsqu'un employé quitte l'entreprise, il perd automatiquement tous ses droits d'accès (voir [ci-dessous](#)),
- Les mots de passe doivent respecter la politique de mots de passe de SBS,
- La politique sécurité interdit à l'employé de divulguer ses informations d'authentification,
- L'accès au système est bloqué après un certain nombre de tentatives d'authentification échouées, comme défini dans la PSI,
- Les utilisateurs sont déconnectés après une certaine période d'inactivité,
- Les droits d'accès des employés ne sont pas transférables,
- Maintenir le nombre de personnes ayant des privilèges administratifs au minimum,
- 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,
- Revoir les privilèges au moins deux fois par an,
- L'accès aux informations et aux systèmes d'information se fait par des canaux chiffrés,
- L'authentification multi-facteurs (MFA) pour les utilisateurs de SBS est obligatoire pour se connecter à un environnement client.

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

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 (plus précisément le même jour à minuit).

8.2.4. Revue des droits d'accès

Des revues sont réalisées sur les droits d'accès des Runs Managers et des droits sur les IBMi au minimum une fois par an.

La fréquence est ajustée en fonction du périmètre et des exigences SSI

8.3. Gestion des comptes utilisateurs du Client

8.3.1. Gestion des droits d'accès des utilisateurs du Client

Dans le cas où l'application permet l'accès à des fonctionnalités par les utilisateurs du Client, la gestion des utilisateurs du Client et de leur niveau de droits est de la responsabilité du Client. Sur demande, la liste des accès peut être fournie au Client. La gestion (création/modification/suppression) doit être effectuée par une demande à SBS. Le compte utilisateur du Client et son mot de passe sont communiqués par SBS de manière sécurisée.

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.). Les utilisateurs du Client n'ont accès qu'aux tickets du site auquel ils sont rattachés (un site peut correspondre à plusieurs filiales).

8.4.2. Authentification et mot de passe

L'authentification pour les utilisateurs de SBS est basée sur les règles de l'Active Directory. Sur demande, il sera possible de fournir les règles à jour sur la gestion des mots de passe. Les modalités d'accès peuvent évoluer en fonction des besoins exprimés par SBS.

8.4.3. Attribution / modification des droits d'accès

Lorsqu'un nouvel employé arrive, un compte est créé et un profil lui est attribué correspondant au poste. Une revue des droits d'accès est effectuée régulièrement.

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

Le verrouillage du compte de l'AD bloquera l'accès à l'outil de ticketing.

9. Sécurité physique

9.1. Sécurité physique dans les locaux de SBS

L'organisation du Groupe 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 sites du Groupe utilisent le système de contrôle d'accès par badge centralisé recommandé par le Groupe. Ce système est utilisé pour restreindre l'accès aux locaux du Groupe 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,
- 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 l'infrastructure critique du 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 Département Immobilier & Achats 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 un responsable de site,
- Le Document de Sécurité de l'Infrastructure du Site (« DSIS ») résume ces exigences pour chacun des sites du Groupe.

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 le Groupe (ou SBS par exception).

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 :

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

9.2. Site de Datacenter

Les Données Clients gérés par SBS pour l'offre SAB en services managés sont hébergées sur deux datacenters. La localisation et les spécificités de ces derniers sont décrits ci-après :

- **Equinix (PA6) est le datacenter de production utilisé par SAB SaaS :**

- Situé à Aubervilliers, France
- Bâtiment de 4901m²
- Certifié ISO27001, ISO 9001, ISO14001, ISO 22301, ISO50001, OHSAS 18001, PCI-DSS, HAD-HADS, SOC 1 et 2 types 2.
- Sécurité d'accès : Entrée double porte avec accès biométrique, Agent de sécurité présent 24/7, Détecteurs de mouvement et vidéo-surveillance

- **Datexion est le datacenter de backup utilisé par SAB SaaS :**

- Situé à Trappes, France
- Bâtiment de 1200m²
- Certifié ISO27001, ISO9001
- Sécurité d'accès : Accès biométrique, agent de sécurité la semaine, vidéo surveillance avec 29 jours de rétentions.

En complément : Sauf indication contraire dans le Contrat, un changement de localisation du datacenter avec le même niveau de sécurité est possible sur décision de SBS : dans ce cas, une information sera fournie au Client. La nouvelle localisation restera conforme aux obligations du Client et à la réglementation locale. Les données du Client sont stockées dans des datacenters situés dans l'Union Européenne.

9.3. Site d'Archive des Sauvegardes

- Hébergement des sauvegardes : Prestataire Iron Mountain situé en France. (Certifiés ISO27001)
Les bandes sont conservées en un (1) exemplaire dans les locaux du prestataire Iron Mountain.
- Le transport des bandes est effectué de manière sécurisée par le Prestataire Iron Mountain dans des véhicules banalisés et surveillés par un système GPS.

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 la PSI de SBS. Cette dernière spécifie le processus d'escalade, les personnes à contacter et à tenir informées, et la formation de l'unité 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 après escalade.

Dans le contexte de SBS, la gestion des incidents de sécurité est décrite dans la procédure d'incident de sécurité de SBS. 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 service est informé par les équipes de la ligne de service de chaque incident de sécurité. Les incidents de sécurité seront présentés au Client selon ce qui a été convenu dans le Contrat.

Tous les incidents de sécurité de l'information affectant SBS et/ou les services externalisés 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 est partagée sur demande. La procédure contient des informations concernant la notification, les descriptions, les remédiations et les leçons apprises.

Les événements de sécurité (non encore officiellement déclarés comme incidents) peuvent être envoyés au CISO du Client si les informations sont suffisantes pour établir une communication directe.

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 de production « brûlant » ou 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 service dès que possible.

En cas d'incident de sécurité, SBS appliquera tous les moyens pour collaborer avec le CISO du Client, 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

De plus, l'analyse de l'origine des incidents de sécurité récurrents, l'identification et la mise en œuvre des mesures de résolution finale des problèmes de sécurité font partie de la gestion générique des problèmes (pour tous types d'incidents) mise en place par SBS.

10.6. Incidents de Données à Caractères 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 dès que possible et suivent les exigences réglementaires.

Si l'incident implique des données personnelles, des informations supplémentaires doivent être communiquées au DPO du Client et au DPO de SBS. L'adresse e-mail du DPO de SBS est : GDPR.ACCESS@sbs-software.com

10.7. Signalement

Tous les employés et sous-traitants doivent signaler ces problèmes au point de contact dès que possible pour éviter les incidents de sécurité de l'information. Le mécanisme de signalement doit être aussi simple, accessible et disponible que possible. Par conséquent, le signalement des incidents de sécurité se fait via l'application de gestion des services informatiques, 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 des activités des Services.

SBS s'efforcera de maintenir le niveau de service défini dans le Contrat et de protéger les processus métier critiques des effets d'une défaillance ou d'une catastrophe 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 un document décrivant les mesures de son Plan de Reprise d'Activité.

11.1. Test du Plan de Continuité des Activités (PCA)

En répondant aux critères des scénarios de risques identifiés, les équipes opérationnelles effectuent un test annuel de leur Plan de Continuité des Activités.

Les résultats de cet exercice et la documentation associée peuvent être mis à disposition sur demande. Les tests sont effectués au niveau des équipes opérationnelles.

(Exemple de scénario : Indisponibilité du site principal).

11.2. Test du Plan de Reprise d'Activité (PRA) des environnements

Pour assurer la résilience de la Solution et permettre l'efficacité de la Solution de sauvegarde de l'infrastructure mise à disposition du Client, un exercice est effectué chaque année. Le test du PRA est planifié et organisé par les équipes en charge de la Solution.

En fonction de la nature de la Solution, les tests du PRA peuvent être effectués sur un environnement de contrôle. Les résultats de cet exercice et la documentation associée peuvent être fournis annuellement sur demande.

11.3. Test du plan de continuité d'activité des prestataires

Afin de s'assurer de la continuité de nos sous-traitants et plus spécifiquement des prestataires critiques (voir Prestataires critiques), SBS reçoit de ses prestataires critiques les résultats des exercices.

Le résultat de ces exercices et la documentation associée peuvent être communiqués annuellement sur simple demande (en fonction de la nature de classification du/des documents, les documents peuvent être « tronqués »).

12. Chiffrement et gestion des secrets

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 l'informatique interne est actuellement Bitlocker). SBS s'engage à utiliser des protocoles de chiffrement robustes sans vulnérabilités connues.

Serveurs des services managés SAB

Par défaut, les données sur les serveurs et baies de stockages ne sont pas chiffrées.

Support magnétique (bande de sauvegarde):

En option, les Données Client sur les bandes de sauvegarde peuvent être chiffrées.

12.4. Chiffrement des données en transit

Par défaut, seuls les protocoles chiffrés sont autorisés entre les différents VLAN, les serveurs doivent utiliser des protocoles chiffrés (SFTP, Https, Pesit SSL, EBICS T et TS).

Si lors de la revue des matrices des flux sont en clair, une fiche de dérogation sera établie avec l'accord de l'ISO de la ligne et présenté lors des comités de Sécurité.

Une PKI interne existe, gérée par l'équipe d'Infrastructure Management de SBS.

Protocole

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 R&D.

12.5. Gestion des secrets

SBS s'engage à garantir que les secrets (par exemple, mots de passe, clés d'accès, clés cryptographiques, certificats, clés de chiffrement, etc.) sont correctement protégés.

Par défaut, nous appliquons les règles suivantes :

- Les secrets ne doivent pas être codés en dur.
- Les secrets ne doivent pas être stockés dans des fichiers en texte clair.
- Les secrets ne doivent jamais être partagés sans protection (chiffrés).
- Les secrets doivent expirer (généralement annuellement).

Plusieurs moyens techniques peuvent être mis en place pour garantir qu'un système de gestion des clés (KMS) ou un coffre-fort approuvé est implémenté pour stocker et gérer les secrets. L'accès au KMS ou au coffre-fort est protégé et restreint à un nombre limité d'utilisateurs autorisés.

Les délais d'expiration sont définis en fonction de la criticité des secrets.

13. Sécurité des opérations de service

13.1. Procédure et responsabilités opérationnelles

13.1.1. Procédures et responsabilités opérationnelles

Les procédures opérationnelles doivent être documentées et mises à la disposition de tous les utilisateurs concernés.

Ces procédures ne sont pas partagées avec le Client mais peuvent être présentées lors d'un audit.

13.1.2. Compétences

Le personnel est formé et sensibilisé aux différents processus et normes de SBS qui leur permettent de comprendre les processus métier et opérationnels (par exemple, ITIL).

13.2. Sauvegarde

SBS s'engage à sauvegarder, conformément aux règles définies par défaut dans cette Annexe, toutes les Données du Client transmises, téléchargées ou stockées sur ou vers l'Infrastructure et SBS sera responsable de la restauration, en utilisant la dernière sauvegarde effectuée, de toutes les données, fichiers ou informations perdus ou modifiés.

13.2.1. Politique standard

Dans le cadre de l'offre SAB en services managés, SBS décrit, ci-après, l'ensemble des services de sauvegarde/restauration mis en œuvre pour ses services.

Il est précisé le périmètre, les moyens, les principes généraux, les types de sauvegarde et les services associés. Les sauvegardes des actifs nécessaires à la réalisation des services managés (logiciels/infrastructures/base de données) sont placées sous la responsabilité de SBS.

La politique de sauvegarde est la suivante :

Fréquence	Contenu	Rétention
Journalière	Toute donnée (data + programmes)	4 semaines sur library optique (VTL)
Mensuelle	Tout le système + toute donnée (data et programmes)	Période glissante sur 10 ans

Les sauvegardes mensuelles sont transférées sur supports Ultrium (LTO) et externalisées de manière sécurisée par le prestataire spécialisé.

13.2.2. Test de restauration

Il est prévu annuellement un (1) Test de restauration à la demande du Client, les tests sont établis sur la base d'une restauration d'une bande mensuelle archivée.

Ils permettent de valider:

- La bonne nomenclature d'une bande
- Le délai de récupération d'une bande
- La procédure de restauration
- Le contrôle de la date de sauvegarde (date des objets)

La preuve du résultat de la restauration de trois (3) objets de la bande sera transmise au Client. Les objets sont indiqués dans le rapport.

SBS réalise mensuellement (i) une sauvegarde des bandes de façon automatique lors des OPTION 21 (sauvegarde complète), (ii) une restauration de 3 objets et (iii) un DSPTAP permettant de s'assurer de la conformité de la bande. Le rapport peut être livré à la demande du Client par exemple dans le cadre des audits.

13.3. Gestion des changements

Pour tout changement impactant la sécurité, l'ISO sera informé. Les opérations effectuées sur les environnements du Client sont sous la responsabilité des équipes d'opérations de SBS en termes de gestion et de déploiement. En cas de maintenance planifiée nécessitant une interruption de service, le Client est informé à l'avance, comme décrit dans le Contrat. Toute intervention en production est testée dans un environnement d'acceptation et/ou de test au préalable.

13.4. Séparation des environnements

Les environnements de production et non-production (PROD, UAT, test, ...) sont séparés pour réduire le risque d'accès non autorisé ou de modifications dans l'environnement de production.

Sauf demande explicite du Client, les données de production ne doivent pas être copiées dans les environnements non-production. En cas de copie dans l'environnement non-production, cet environnement doit avoir des mesures de sécurité équivalentes à celles du système de production.

Le cloisonnement par différentes zones de sécurité (VLAN) notamment pour l'administration est nécessaire afin de limiter la propagation des attaques.

Il est associé aux fonctions de filtrages gérées par les pare-feux.

Tous les flux externes ainsi que les flux d'administration et de télémaintenance sont filtrés par un pare-feu.

Aussi hors cas spécifique, nécessitant un traitement spécifique, les données des environnements de recette et de test ne sont pas pseudonymisées (au sens du RGPD).

Environnement de R&D :

Pour rappel : les environnements Clients Production, recette, test sont des environnements hébergés dans Cloud Privé SBS. Aucun environnement de R&D n'est créé par duplication des environnements Clients et les environnements de R&D ne contiennent aucune Donnée.

Administration et VLAN :

L'administration de l'ensemble des équipements au sein de l'Infrastructure informatique est réalisée au travers d'un réseau dédié isolé (VLAN d'administration). Ce dernier n'est accessible qu'aux seuls administrateurs.

Dans le cadre des mesures de sécurité liées à la réduction de privilèges, confidentialité, traçabilité, SBS proposera une solution d'accès distant pour administrateurs et personnel support.

L'authentification des administrateurs de SBS aux zones d'administration fait déjà l'objet d'une authentification à double facteur.

Les accès aux équipements gérant les flux d'administration sont assurés par des connexions VPN IPSEC L2L entre les sites localisant les administrateurs et les Datacenters.

Les moyens d'accès aux équipements administrés :

- Les accès aux équipements administrés sont assurés via des protocoles sécurisés (exemple : SSH, Https, Telnet-ssl)
- Les accès aux équipements font l'objet d'une politique de filtrage firewall spécifique identifiant chaque administrateur et flux autorisés (ports/applications)
L'utilisation de connexions chiffrées est une priorité en cas de mode dégradé, une dérogation de sécurité sera créée avec une date de retour vers le mode nominal.

13.5. Protection contre les logiciels malveillants

La gestion des antivirus est valable uniquement pour les systèmes d'exploitation Windows (serveurs et ordinateurs portables) (cf. ce point est décrit dans chaque produit de la Solution).

Les antivirus et EDR sont déployés sur tous les postes de travail des employés de SBS (le logiciel actuel est Microsoft Defender).

Les antivirus et EDR sont déployés au minimum sur tous les systèmes d'exploitation Windows de la Solution, et certains environnements Linux (le logiciel actuel est WithSecure).

La surveillance des antivirus est effectuée par les équipes opérations IM et présentée au comité de sécurité de SBS en cas de défaillance ou si le comité de sécurité nécessite des informations (écart de fonctionnement, etc.).

13.6. Journalisation et suivi

13.6.1. Synchronisation de l'horloge NTP

Des réglages d'horloge corrects sont essentiels pour garantir des journaux d'audit précis qui peuvent être utilisés dans des enquêtes ou comme preuves dans des affaires judiciaires ou des procédures disciplinaires. Des journaux d'audit inexacts peuvent entraver les enquêtes et nuire à la crédibilité des preuves. Pour les systèmes de journalisation, une horloge maîtresse connectée à un signal horaire diffusé par une horloge atomique nationale peut être utilisée.

Le protocole NTP garantit que tous les serveurs sont synchronisés avec l'horloge maîtresse. Il peut y avoir plusieurs serveurs de temps en fonction de l'utilisation (pare-feu / serveurs).

13.6.2. Traçabilité IBMi

En option, lorsque le Client souscrit à ce service de traçabilité, pour les serveurs IBM (Cœur de la solution SAB), SBS veille à employer une solution partenaire d'audit et contrôle d'accès.

La tables des habilitations peut être journalisée et auditée (rapport sur les changements) via une solution partenaire (de type Precisely AssureSecurity) :

- Modifications de tout compte utilisateur de l'environnement IBMi, modifications des habilitations, modifications des paramètres systèmes IBMi, tout accès aux serveurs IBM
- Tous les accès techniques aux serveurs IBM sont contrôlés, quel que soit le protocole utilisé, et les accès sont traçables dès lors qu'ils sont autorisés – compte administrateur, compte de service, compte utilisateur :

Des pistes d'audit applicatives SAB, par domaine, (archivages base de données) peuvent être paramétrées et mises en œuvre. (Ex. sur des transactions moyens de paiements, validations,)

En option : tous les composants IBMi, dédiés au Client, peuvent alimenter un SIEM¹ (avec un SOC).

13.6.3. Serveurs et Equipements réseaux

Tous les serveurs, équipements réseaux gérés par –SBS au titre de l'offre SAB en services managés produisent des journaux.

13.6.4. Journaux d'application

Les journaux d'application sont des journaux générés par les applications de la Solution. Les journaux sont essentiels pour l'analyse en cas d'incident, mais le niveau de détail et le volume en production ne doivent pas être une contrainte pour le bon fonctionnement de la Solution.

¹ SIEM (Security Information and Event Management)

13.7. Gestion des compétences pour l'exploitation des logiciels

Toutes les opérations affectant les systèmes sont effectuées par des opérateurs formés et qualifiés en ce qui concerne le processus de changement. L'opérateur est clairement identifié et suit une formation régulière pour mettre à jour ses connaissances.

13.8. Service SOC-SIEM

a. Event Processor » et gestion des logs :

Par défaut, au minimum les logs des Firewalls sont conservés sur un équipement appelé « Event Processor » pendant douze mois glissants.

b. Option SOC-SIEM :

Deux niveaux sont disponibles, afin de répondre aux enjeux suivants :

- Se prémunir contre les attaques avancées actuelles (dont les ransomwares)
- Amélioration des détections des attaques
- Réponse aux nouvelles typologies d'attaque
- Répondre aux nouvelles exigences sécurité du Groupe Sopra-Steria et du CISO SBS.
- Augmenter le niveau de sécurité

Le SOC-SIEM mis en place par SBS suit les bonnes pratiques recommandées par l'ACPR permettant de disposer d'un outil de traces (avec une rétention de douze mois glissante) ainsi que d'une équipe de surveillance pour les exploiter en 24h/24 et 7j/7 via Sopra-Steria Cyber.

13.9. Gestion des correctifs

13.9.1. Gestion des correctifs des postes de travail et serveurs gérés par le département informatique.

La gestion des correctifs de sécurité est appliquée aux postes de travail et serveurs gérés par le département informatique. Dans le cadre de la mise en œuvre des mesures de sécurité, la gestion des correctifs de sécurité sur les postes de travail des administrateurs et sur les serveurs fournissant des services aux clients est sous la responsabilité de SBS.

13.9.2. Gestion des correctifs de l'infrastructure de l'environnement client de SBS

Catégorie	Contenu
Windows	Les mises à jour sont réalisées en deux étapes (Recette) et (Prod) et réalisés via Wsus
Linux	Les mises à jour sont réalisées en deux étapes (Recette) et (Prod) et réalisés via l'outil de type Spacewalk (ou équivalent)
IBM I	Mise à jour réalisés à minima 1 fois / an
Infrastructure de Sécurité & Réseau	Mise à jour manuellement au moins 2 fois / An
Logiciels infrastructures	Mise à jour réalisée 1 fois / an

En complément, pour le Progiciel et les serveurs, les mises à jour majeures sont réalisées en fonction des prérequis éditeur SBS et des mises à niveau demandé par les éditeurs tiers (tels que IBM).

Les logiciels d'infrastructures utilisés dans le cadre du Contrat sont maintenus à jour par SBS. Dans le cas contraire, une dérogation doit être demandée, elle doit être justifiée et validée conjointement avec la SSI SBS et la SSI du Client.

Le mode opératoire induit un ensemble de TNR (Tests de Non-Régressions) en relation avec le Client.

Les versions majeures peuvent faire l'objet d'une validation du Client qui devra également s'assurer du bon fonctionnement du Progiciel.

Point important : Dans le cas spécifique où le Client n'a pas mis en production la dernière version du Progiciel SAB éditée par SBS, SBS ne prend pas les engagements sur la gestion des vulnérabilités (chapitre suivant) et la maîtrise des middlewares décrits ci-après.

La SSI indiquera l'obsolescence des versions et des middlewares lors des comités de sécurité afin de procéder aux Security Exceptions.

13.9.3. Gestion des correctifs des applications

En ce qui concerne les Offres SBS, cela est indiqué dans le QAP (Plan d'Assurance Qualité)

13.10. Gestion des vulnérabilités

13.10.1. 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.

13.10.2. 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 français

La gestion des alertes CERT est basée uniquement sur les alertes indiquées comme Élevées ou Critique. L'impact des vulnérabilités peut varier en fonction de plusieurs paramètres, tels que l'exposition de l'actif concerné et son environnement. L'ISO de la ligne de service est responsable de l'évaluation et du recalcul du score de vulnérabilité et de la définition des priorités de P1 à P4. Seules les vulnérabilités classées P1 et P2 sont gérées directement, avec un délai de traitement établi à partir de la confirmation interne de l'alerte (suivant la date de publication du CERT). Si le délai n'est pas respecté, l'ISO doit être consulté.

Les rapports d'alerte CERT sont analysés par l'ISO de la ligne de service. Toutes les alertes CERT P1 et P4 sont examinées et présentées au comité de sécurité ou COMSEC

Catégorie	Délai de traitement
P1 - Critical	Délai de traitement : 1 semaine
P2 - High	Délai de traitement : 3 semaines pour les services exposés Délai de traitement : 6 semaines pour un service non exposé (exemple : VPN) Délai de traitement : 26 semaines si l'actif n'est pas considéré à risque.
P3 - Medium	Géré par les processus standard (business as usual)
P4 - Low	Géré par les processus standard (business as usual)

13.10.3. Scan des vulnérabilités par les équipes d'opérations

Le service de surveillance des vulnérabilités prévoit :
Des analyses de vulnérabilités périodiques effectuées sur les actifs identifiés dans le service client (fréquence de périmètre adaptée à chaque ligne, au moins tous les mois (avec un rapport interne et présenté par l'ISO lors du comité de sécurité). Outils utilisés : AWS Inspector, CyberWatch, ou Qualys ou équivalent.

Optionnellement, un rapport trimestriel, dédié au Client, peut être fourni.

L'impact des vulnérabilités peut varier. En fonction de certains paramètres tels que l'exposition de l'actif concerné, son environnement, ... L'ISO de la ligne de service pourrait réévaluer ou recalculer le score CVSS ou le score interne de l'outil d'analyse et définir une priorité/catégorie P1 à P4.

Catégorie	Délai de traitement
P1 – Critical	Délai de traitement : 1 semaine
P2 – High	Délai de traitement : 3 semaines pour les services exposés Délai de traitement : 6 semaines pour un service non exposé (exemple : VPN) Délai de traitement : 26 semaines si l'actif n'est pas considéré à risque.
P3 – Medium	Délai de traitement : 26 semaines
P4 – Low	Délai : à convenir avec la ligne de service en fonction de la complexité du coût, du risque. Souvent intégré dans la mise à jour de version. Les actions considérées à long terme sont des Security Exception

Une Security Exception est soulevée si le délai défini ci-dessous n'est pas ou ne peut pas être respecté. Pour rappel, si le package logiciel n'est pas à la dernière version, la gestion des vulnérabilités permet de déterminer si des composants sont devenus obsolètes ou vulnérables.

13.11. Connexions aux environnements du Client

Connexion depuis SBS

À la suite d'une déclaration d'Incident par le Client ou à la suite d'une opération de maintenance, des connexions aux environnements sont nécessaires.

Les accès aux environnements de production par les équipes Supports N1/N2 sont effectuées par l'intermédiaire d'un « Jump Server » (serveur de rebond) : Un serveur Wallix (accès nominal) et un accès via une machine de rebond (Solution dégradée) à même de journaliser les actions opérées sur les systèmes Clients.

La procédure de connexion appliquée aux interlocuteurs SBS des équipes R&D et/ou du Support : Une demande de connexion est réalisée via l'outil de ticketing puis validée par l'équipe en charge des services managés SAB. Les informations de connexion sont transmises après validation à la personne qui a initié la demande.

13.12. Outil de télémaintenance sur le Progiciel

SBS livre régulièrement des maintenances correctives et réglementaires, ou des « releases » du Progiciel et/ou de la Solution.

Ces maintenances se font par transmissions sécurisées vers le site d'hébergement des infrastructures.

Ces programmes, fichiers, sont réceptionnés dans l'outil de télémaintenance du progiciel qui permet ensuite de les intégrer automatiquement sur les différents environnements du Client, selon le rythme choisi et l'organisation des mises en œuvre.

La console de télémaintenance permet de tracer les différentes installations sur les environnements de la Solution. La console permet aussi à la maintenance de connaître le niveau de version du Progiciel et de la liste précise des TLM (télémaintenances installées).

14. Sécurité du développement

14.1. Cycle de vie du développement logiciel sécurisé

Les logiciels développés par SBS sont soumis aux règles du Plan d'Assurance Sécurité de l'Éditeur (e-SMP). Ce dernier définit les exigences de sécurité pour les activités de développement et principalement les points suivants :

- Bonnes pratiques en matière de sécurité et de développement sécurisé
- Intégration et révision des frameworks
- Prise en compte des directives OWASP TOP 10.

Traitement des recommandations suite aux audits réalisés par SBS et les auditeurs SECAPP SBS.

L'objectif est de garantir, par des contrôles réguliers, que les Offres SBS déployées ne contiennent aucune vulnérabilité critique.

En plus de ces contrôles, des tests d'intrusion peuvent être effectués par l'entité de cybersécurité de Sopra Steria pour s'assurer qu'aucune vulnérabilité critique n'est présente dans l'environnement. Ce service peut être fourni sur demande et fera l'objet d'un devis.

14.2. Gestion des logiciels open-source

La gestion des logiciels open-source intégrés dans nos logiciels est directement surveillée par notre département R&D, suivant les directives d'un « Livre des règles de licence », documentation qui définit les règles régissant l'utilisation des licences de type GPL2, par exemple, et la gestion des vulnérabilités et de la dette détectées par nos outils de contrôle SBOM.

Les contrôles sont effectués dans le cadre des KPI de SBS et dans le suivi des mises à jour de version par les Responsables de la Sécurité.

15. Relations avec les fournisseurs

Les fournisseurs critiques sont identifiés selon les directives de l'EBA. Le suivi des fournisseurs est effectué par la ligne de service et l'équipe des opérations.

La liste des fournisseurs critiques dépend de la Solution fournie.

Nom	Périmètre / Relations / Suivi
Equinix	Datacenter Contrat signé entre SBS et le prestataire ISO27001 – ISAE3402
Dataxon	Datacenter Contrat signé entre SBS et le prestataire ISO27001
Iron Mountain	Archiviste bande sauvegarde Contrat signé entre SBS et le prestataire ISO27001
SOPRA STERIA POLSKA	Prestataire réalisant des actions d'Opération Management Contrat signé entre SBS et le prestataire ISO27001
SOPRA STERIA INFRASTRUCTURE & SECURITY	Gestion de la Sécurité SOC-SIEM PASSI / PRIS (on-going)

Dans le cas d'un remplacement ou d'un ajout d'un prestataire critique, SBS informera le Client avant la prise de fonction du prestataire.

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.

16.2. Mesures

Les mesures en place doivent prouver leur efficacité. La performance de la sécurité est mesurée au sein des opérations par la formalisation d'objectifs et d'indicateurs associés qui sont rapportés par le CISO de SBS à la Direction Générale.

Le département des opérations surveille les éléments suivants pour se conformer aux exigences :

- Suivi par le comité de sécurité mensuel dédié à la ligne de service pour tous les clients.
- Suivi dans les comités de risque IAM.
- Surveillance via le plan de conformité annuel de la sécurité de l'information de SBS. Les indicateurs incluent la surveillance des plans de scan de vulnérabilité, de continuité, d'audits, de formation et de suivi des P1 identifiés dans les audits, ces indicateurs sont revus annuellement.

- Surveillance hebdomadaire de la ligne 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

En fonction de la portée, des indicateurs de sécurité sont établis et surveillés par l'ISO de la ligne 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
- Charte d'utilisation des équipements informatiques
- Politique de gestion des comptes (comptes administrateurs et de service, politique de mots de passe, etc.)
- Note interne annuelle sur l'organisation de la Sécurité de l'Information
- DSIS du site pour chaque local.

18. Abréviations et acronymes

Abréviation	Définition
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.
DRP	Plan de Reprise d'Activité
SMP	Plan de Gestion de la Sécurité
ISP	Politique de Sécurité de l'Information
CISO	Chief Information Security Officer
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CAB	Change Approval Board
CERT	Computer Emergency Response Team
CNIL	Commission Nationale de l'Informatique et des Libertés
COMSEC	Comité de Sécurité
COPIL	Comité de Pilotage
MM	Minutes de Réunion
PD	Données Personnelles
GM	Directeur Général
DI	Département Industriel
DID	Directeur du Département Industriel
DOD	Directeur des Opérations
DPO	Data Protection Officer
IT Dep	Département Informatique
F2F	Face2Face - Intranet d'entreprise
I/O	Input/Output
ITIL	Information Technology Infrastructure Library
RACI	Matrice Responsable-Accountable-Consulted-Informed
ISO	Information Security Officer
DSIS / SISD	Dossier de Sécurité Infrastructure Site
IAM	Internal Approbation Meeting
Run manager	Responsable de l'Accord et des opérations pour le Client
Vulnérabilité	Une faiblesse d'un actif ou d'un groupe d'actifs qui peut être exploitée par une ou plusieurs menaces
SBS	SBS Software, une filiale de 74 Software Group

Customer	Le client qui a souscrit à la fourniture de la Solution comme stipulé dans l'Accord
Solution	Désigne la combinaison de (i) les Offres SBS ; et (ii) l'Infrastructure
MFA	Multi-Factor Authentication – Authentification multifacteur
NTP	Network Time Protocol – Protocole de synchronisation de l'heure
TLS	Transport Layer Security – Protocole de sécurisation des communications
VPC	Virtual Private Cloud – Réseau privé virtuel dans le cloud AWS
KMS	Key Management Service – Service de gestion des clés de chiffrement
SBOM	Software Bill of Materials – Inventaire des composants logiciels
OWASP	Open Web Application Security Project – Projet de sécurité des applications web
CVSS	Common Vulnerability Scoring System – Système de notation des vulnérabilités
BYOD	Bring Your Own Device – Utilisation d'appareils personnels au travail
PRA	Plan de Reprise d'Activité
PCA	Plan de Continuité des Activités
DLP	Data Loss Prevention – Prévention contre la perte de données
R&D	Recherche et Développement
ITSM	IT Service Management – Gestion des services informatiques
SI	Système d'Information
AV	Antivirus
IM	Infrastructure Management
SOC	Security Operations Center
OS	Operating System
MS	Microsoft
USB	Universal Serial Bus
NDA	Non-Disclosure Agreement
UAT	User Acceptance Testing
NIST	National Institute of Standards and Technology
IEC	International Electrotechnical Commission
EBS	Elastic Block Store (AWS)
AES	Advanced Encryption Standard
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
VPN	Virtual Private Network
PROD	Environnement de Production
COMSEC	Comité de Sécurité
KPI	Key Performance Indicator
EBA	European Banking Authority
SECAPP	Security Application Audit (interne SBS)
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité (ANSSI)