# Plan d'Assurance Sécurité Cloud SBS SaaS

SBS SaaS Security Management Plan_(fr)_v17032025

# Table des matières

# 1. Présentation du Plan d'Assurance Sécurité

Ce Plan d'Assurance Sécurité (« PAS ») est intégré et complète le Contrat conclu entre le Client et SBS. Ce document décrit les mesures de sécurité, l'organisation et les processus mis en place par SBS dans le cadre de la fourniture des Services. Ce PAS est valable sur les environnements de production et non-production du Client opérés sur l'infrastructure AWS. Certains indicateurs de sécurité ou exigences techniques peuvent être adaptés en fonction de leur criticité et de leur exposition. 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. Les demandes spécifiques de réversibilité font l'objet d'une proposition commerciale, SBS maintenant des processus de réversibilité documentés.

# 3. Audit de sécurité

SBS réalise des audits de sécurité réguliers, adaptés à la ligne de service et à la portée spécifiques. 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 globale

SBS est responsable des procédures de sécurité de ses sous-traitants. Des contrôles réguliers sont mis en place par SBS pour vérifier la conformité de sécurité de ces sous-traitants. (Contrôle minimum : Chaque année pour respecter la certification).

# 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 eut 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. 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 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 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 service.** L'Officier de la Sécurité de l'Information (« ISO ») sera affecté spécifiquement à la ligne de service et spécifiquement au Client. Il ou elle sera nommé(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 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 l'Unité d'Affaires (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 nos produits et les plans de remédiation associés
- Identifier les activités nécessitant une certification (en particulier ISO/IEC 27001), puis assister à la mise en œuvre des projets de certification et à leur suivi annuel
- Participer activement aux communautés de sécurité
- Signaler tous les incidents et problèmes de sécurité.
- Participer aux « communautés de sécurité externes » et ainsi 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

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 est revue annuellement. Les critères d'évaluation des risques de sécurité au sein de la ligne de service sont définis par l'ISO. Leur principal objectif est d'établir des niveaux de risque acceptables. Les risques résiduels sont soumis et acceptés par la direction de la ligne de service.

L'analyse des risques fait partie intégrante de la gouvernance de la sécurité de SBS. Elle est réalisée de manière continue entre les équipes de maintenance opérationnelle 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 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 cours de formation traitent des sujets suivants : (i) Bases de la sécurité pour tous, (ii) Bases de la sécurité pour les chefs de projet, (iii) Sécurité dans les développements (formation dispensée en fonction du rôle/fonction de l'employé), (iv) Protection des données, (v) Sensibilisation à la corruption, (vi) Campagne annuelle de test de prévention du phishing.

**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 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 et qualifiées.
Les règles de classification de l'information (procès-verbaux, 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 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 :

- Stocker tous les documents classifiés dans une armoire verrouillée.
- 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 avec le câble de sécurité fourni par le département informatique lorsqu'il n'est pas sous une surveillance directe.
- Garder l'ordinateur portable avec l'employé.
- Attacher l'ordinateur portable et le mettre en sécurité pendant toute absence (soirées, week-ends, vacances).
- 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 doivent être émises pour la gestion de ces supports physiques externes. Dans le cadre d'un audit, le Client peut demander à SBS de transmettre ces règles pour vérification, afin de valider le niveau de sécurité des supports 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 le Guide de gestion de la documentation du Système de Qualité (SQ). Cet aspect est régi par la politique de sécurité « Gestion des actifs », chapitre 4 « 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,
- Dans le Guide de gestion de la documentation pour la classification des documents,
- Dans le document de politique de « Classification de l'information » de SBS, qui décrit les différents cas d'utilisation,

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.

<u>Destruction de l'information :</u>

Lorsque l'information n'est plus nécessaire, des moyens sont mis à disposition des employés de SBS pour la détruire. Cela inclut le processus de gestion des vulnérabilités ou de l'obsolescence des équipements :

- Déchiqueteuse pour les documents papier,
- Procédure de gestion de l'obsolescence et des exceptions pour l'infrastructure,
- Sur AWS, les disques sont chiffrés et détruits lorsqu'ils sont mis hors service :
    - Tous les volumes AWS EBS utilisés pour stocker des données sont, en plus d'être chiffrés avec une clé gérée en dehors du volume par AWS KMS, effacés avant toute réutilisation.
    - La mise hors service des disques est décrite dans le livre blanc « AWS: Overview of Security Processes » section « Storage Device decommissioning » (https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf) qui explique que les disques en fin de vie sont effacés puis détruits conformément à la norme NIST 800-88.
- Une procédure est déployée par les équipes de gestion de l'infrastructure pour la mise hors service.

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

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 AWS 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 ralenti puis 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

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

Les revues d'accès sont déterminées en fonction de la portée (administrateurs, utilisateurs, etc.) et décrites dans la documentation technique de chaque produit.

### 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

Amazon Web Services a reçu diverses certifications d'organismes tiers. Les rapports et certificats sont disponibles pour tous les clients d'AWS sous NDA via leur service AWS Artifacts. Ces certifications incluent SOC 1, SOC 2, SOC 3, ISO 27001, HIPAA et HITECH. Ces documents peuvent être consultés via https://us-east-1.console.aws.amazon.com/artifact/reports/aws (nécessite un compte AWS). Conformément à la politique de confidentialité d'AWS, il n'est pas possible pour SBS de partager ces rapports. Cependant, toute personne ou organisation disposant de son propre abonnement AWS peut consulter ces documents. Des informations supplémentaires sur la conformité et la politique de sécurité d'AWS sont disponibles sur leur site. Le tableau suivant fournit des liens vers certaines ressources sur ce sujet :

| Titre | Origine | Lien |
|---|---|---|
| AWS Cloud Security | AWS | security |
| AWS Datacenter security | AWS | compliance/data-center/controls |
| AWS Whitepapers | AWS | whitepapers |
| AWS Compliance | AWS | compliance |
| AWS Artifacts | AWS | artifact |

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.

# 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@soprabanking.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 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@soprabanking.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.

## 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 et services AWS
Par défaut, les données sur les serveurs sont chiffrées en utilisant les processus AWS (le chiffrement AES-256 est utilisé, plus de détails sont décrits dans la documentation produit interne).

### 12.4. Chiffrement des données en transit

Par défaut, la mise en œuvre de tout protocole de transfert doit être chiffrée pour les échanges de données entre les VPC (Virtual Private Cloud) et pour les échanges de données entre le VPC de SBS et les clients.
Par défaut, tous les flux réseau sont chiffrés au sein du service VPC (Virtual Private Cloud), sauf en cas de raison technique exceptionnelle. Dans ce cas, une exception de sécurité est soulevée par l'ISO de la ligne de service.

Protocole
Par défaut, seuls les protocoles chiffrés (sFTP, HTTPS, ...) sont autorisés entre les différents VPC.
Cette mesure est obligatoire lorsque des Données Client sont présentes dans l'environnement. 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 des Services convenus avec ses clients, SBS décrit tous les services de sauvegarde et de récupération mis en œuvre pour ses services clients. Il spécifie la portée, les moyens, les principes généraux, les types de sauvegarde et les services associés. Ces services de sauvegarde et de récupération sont basés sur les services AWS dédiés à fournir cette fonctionnalité à toutes les abonnements AWS utilisant les mêmes services. SBS est responsable de la configuration correcte et de la mise en œuvre de ces services AWS. Par conséquent, la sauvegarde des actifs fournissant les services clients (logiciels/infrastructure/base de données) est placée sous la responsabilité de SBS.

Toutes les données (exemple : instances de base de données, fichiers, machines virtuelles, ...) nécessaires au fonctionnement de la Solution en fonction des services doivent être sauvegardées selon la politique de sauvegarde standard.
SBS veille à ce que les sauvegardes des Données du Client soient sécurisées et protégées contre la destruction physique. Les sauvegardes sont stockées de manière sécurisée en utilisant des techniques de chiffrement robustes.

Pour les environnements de production, la politique standard est la suivante :

| Fréquence | Rétention | Type |
|---|---|---|
| Quotidienne | 7 jours | Sauvegarde complète |
| Hebdomadaire | 4 semaines | Sauvegarde complète |
| Mensuelle | 12 mois | Sauvegarde complète |

(*) pas de sauvegarde incrémentielle sur AWS, cela peut être considéré comme une sauvegarde complète.

Dans des cas spécifiques, la ligne de service peut décider de dévier de cette politique standard lorsque la sauvegarde d'un actif n'a pas de valeur ajoutée pour la Solution opérée.

#### 13.2.2. Exceptions

Plusieurs services AWS dévient de cette norme car ils reposent sur les principes de versioning suivants :

**Base de données**

Dans les Solutions opérées utilisant une ou plusieurs instances de base de données ne contenant aucune Donnée Client. La ligne de service peut décider d'adapter la fréquence et la rétention.

**Machines virtuelles**

La politique de sauvegarde ne s'applique pas aux machines virtuelles basées sur des images (AMI) ou des conteneurs de micro-services (exemple : conteneur Docker) ne contenant pas de données persistantes.

**AWS S3**

Il est possible de stocker des données sur un stockage à froid en utilisant AWS S3 (Glacier). Ces données sont stockées sur S3 via des objets. En utilisant le versioning S3 sur ces objets, les données peuvent être préservées, récupérées et restaurées. Une politique de rétention peut être définie pour répondre aux obligations de conformité.

#### 13.2.3. Test de restauration

Chaque année, SBS effectue un test de restauration sur un environnement de référence. Ce test fait partie du rapport annuel de test de DRP.

#### 13.2.4. Archivage

Par défaut, les données archivées concernent les ressources de production de la Solution et sont gérées dans AWS. Si requis par les réglementations, un processus d'archivage optionnel peut être fourni, et cela doit être spécifié dans le Contrat.

### 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.
La ségrégation des zones de sécurité en particulier pour l'administration, est nécessaire pour limiter la propagation des attaques.
En ce qui concerne les mécanismes de séparation des Données du Client dans les environnements AWS, SBS a mis en place des contrôles de sécurité stricts pour garantir l'isolation entre le réseau d'entreprise et les interfaces de gestion et les environnements du Client.

Les mesures de sécurité mises en œuvre, surveillées et révisées sont les suivantes :

- Les activités d'administration et d'exploitation sont effectuées par des utilisateurs SBS authentifiés.
- Les activités d'administration et d'exploitation ne sont possibles que par des employés autorisés par le Delivery Manager.
- Les postes de travail, qui font l'objet d'un contrôle régulier (correctifs OS, signatures AV, ...), sont utilisés pour se connecter aux environnements AWS.
- Les infrastructures SBS construites sur AWS utilisent AWS VPC pour fournir les restrictions réseau et de segmentation nécessaires.
- Certaines interfaces de connexion de produits peuvent être soumises à mTLS, direct connect, ligne louée, VPN ou liste blanche IP...
- Les activités d'administration sont enregistrées et surveillées.

Les environnements R&D ne sont pas gérés par les équipes d'opérations, mais directement par le département R&D. SBS veille à ce que les environnements R&D ne contiennent pas de Données Client, sauf demande explicite du Client.

## 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 Trend Micro-Cloud One).
La surveillance des antivirus est effectuée par les équipes opérations Cloud Ops 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. Suivi des opérations sur AWS.

Toutes les opérations effectuées sur AWS sont journalisées en fonction des besoins des différentes équipes, y compris les équipes d'opérations.

### 13.6.3. 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.

## 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. Gestion des correctifs

### 13.8.1. 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.

### 13.8.2. Gestion des correctifs de l'infrastructure de l'environnement client de SBS

La gestion des correctifs est assurée par les différentes équipes techniques et documentée.
Par défaut, la règle de sécurité est des mises à jour automatiques hebdomadaires pour les correctifs de sécurité dans nos systèmes d'exploitation avec une capacité de correction manuelle en cas d'urgence. En fonction de l'application et de ses prérequis, ces mises à jour peuvent être organisées différemment.

### 13.8.3. Gestion des correctifs des applications

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

## 13.9. Gestion des vulnérabilités

### 13.9.1. 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.

### 13.9.2. 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<br>Délai de traitement : 6 semaines pour un service non exposé (exemple : VPN)<br>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) |

### 13.9.3. 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 mensuel, 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<br>Délai de traitement : 6 semaines pour un service non exposé (exemple : VPN)<br>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.<br>Souvent intégré dans la mise à jour de version.<br>Les actions considérées à long terme sont des exceptions de sécurité |

Une exception de sécurité 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.

### 13.10. Connexions aux environnements du Client

**Connexion depuis SBS**
SBS dispose d'une procédure de gestion des connexions. Les procédures peuvent être présentées lors d'un audit.
Chaque utilisateur dispose de sa propre clé de sécurité ou de ses identifiants personnels sécurisés avec une authentification multi-facteurs et basés sur le gestionnaire de sessions AWS.
Tous les accès au système ne sont possibles que par ce gestionnaire de sessions qui centralise toutes les connexions. Plusieurs sources de journaux et d'événements sont collectées et stockées de manière sécurisée pour constituer une piste d'audit fiable qui suit les connexions effectuées sur la plateforme. Ces pistes peuvent être utilisées pour des audits, des examens ou pour analyser les comportements sur la plateforme.

## 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.

| Fournisseur | Nom du produit ou fonction | Domaine | Description |
|---|---|---|---|
| TINK | TINK | Market Place | DSP2 Use case; PSD2 Bank Act as TPP API PSD2 Bank Act as TPP |
| KOBIL | KOBIL | Market Place | Cas d'utilisation ; Identités numériques sécurisées et communications professionnelles |
| AWS | AWS | Technique | Services techniques cloud |
| MongoDB | ATLAS | Technique | Base de données sur AWS |
| IBM | Safer Payment | Software | Détection de fraude |

## 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. Certification

SBS est actuellement certifié ISO/IEC 27001:2017 pour le périmètre cloud natif. Lors des prochaines révisions, une extension de la portée aura lieu.

### 16.5. 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 Responsible-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 |