Plan d'Assurance Sécurité Silae Global

V3

Dernière révision : 19 décembre 2024

Sommaire

1. OBJET ET DOMAINE D'APPLICATION

Ce document a pour objectif de définir le plan d'assurance sécurité Global pour Silae et les services proposés par l'entreprise. Il vise à répondre aux exigences en matière de sécurité de l'information et de protection des données personnelles, conformément au RGPD.

Les informations, préconisations et normes décrites dans ce document s'appliquent dans tous les cas, sauf si elles sont remplacées par une annexe spécifique liée à un produit ou à un service particulier de Silae.

Ce document pourra être modifié à tout moment sans notification préalable. Les informations renseignées sont l'état de l'art au moment de sa rédaction. Silae est engagé dans une démarche d'amélioration continue et proactive. Les informations, les services exposés sont susceptibles d'évoluer à tout moment pour améliorer la posture de sécurité de Silae.

Silae s'engage à garantir une qualité de service optimale en assurant la disponibilité des applications confiées et en faisant preuve d'une réactivité exemplaire lors de la survenue d'un incident ou de la réception d'une demande client.

Afin de garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité (DICT) des informations, ainsi que leur licéité et leur résilience, Silae met en œuvre une politique de sécurité de l'information. Cette politique détaille l'ensemble des mesures de sécurité et des règles d'hygiène numérique applicables aux activités de l'entreprise.

Cet engagement illustre l'intérêt porté par le groupe Silae à l'adoption de cette politique ainsi que sa volonté de se conformer aux meilleures pratiques en matière de sécurité de l'information et de protection des données personnelles.

Cette politique de sécurité des systèmes d'information s'applique à l'ensemble des moyens humains, techniques et organisationnels mobilisés pour soutenir l'activité de l'entreprise. Elle couvre toutes les opérations de création, de conservation, d'échange et de partage d'informations entre les acteurs internes et externes de Silae, quelle que soit la forme sous laquelle ces informations sont utilisées (électronique, imprimée, manuscrite, vocale, image, etc.), et en particulier :

À l'ensemble des partenaires, clients, utilisateurs ou tiers dès lors que :

- Ils utilisent un ou plusieurs produits Silae
- Ils utilisent le système d'information de Silae
- Leur propre système d'information est relié au réseau informatique de Silae
- À l'ensemble des utilisateurs de l'entreprise dès lors qu'ils effectuent des opérations au travers du système d'information de Silae
- À tous les composants matériels et logiciels d'un système d'information support des activités de Silae
- Aux bâtiments et locaux hébergeant les ressources humaines et les moyens informatiques de Silae

- À l'ensemble des procédures et modes opératoires de production et d'échange d'informations, quelle qu'en soit la nature (données, voix, images)

2. PERSONNELS IMPLIQUES

L'évaluation des risques liés à la sécurité des systèmes d'information est supervisée par le Responsable Sécurité des Systèmes d'Information (RSSI). Cette analyse peut également être initiée en cas de changements majeurs, qu'ils soient organisationnels ou techniques. Par ailleurs, un Délégué à la Protection des Données (DPO) a été désigné pour garantir la prise en charge de tous les aspects relatifs à la protection des données personnelles.

Une fois l'analyse réalisée, les résultats sont communiqués à la direction, qui détermine le seuil d'acceptabilité des risques. Ce seuil est ensuite transmis au Responsable Sécurité des Systèmes d'Information (RSSI), chargé de veiller à son application. Cette décision donne lieu à des actions identifiées et validées dans le cadre du plan de traitement des risques, lequel assure le suivi et la mise en œuvre des initiatives en réponse à l'évaluation des risques.

L'ensemble des collaborateurs est pleinement impliqué dans la démarche de sécurité des systèmes d'information, y compris au-delà du périmètre certifié. La charte informatique incarne l'engagement et la responsabilisation des salariés de Silae. Ce document garantit que chaque collaborateur a connaissance des règles générales à respecter en matière de sécurité des systèmes d'information, notamment dans l'utilisation du matériel qui lui est confié. Cet engagement de confidentialité est formalisé en annexe lors de la signature du contrat de travail de chaque collaborateur.

3. REVUE ET DIFFUSION DE LA POLITIQUE DE SECURITE

La revue et la mise à jour de la politique de sécurité des systèmes d'information sont placées sous la responsabilité du Responsable de la Sécurité des Systèmes d'Information de Silae.

La politique est revue a minima annuellement en prenant en compte :

- Les évènements internes, notamment : modifications des missions de Silae, évolution des structures.
- Les évènements externes, notamment : changement de législation, évolution de la politique contractuelle, nouveaux partenaires.

La politique de sécurité de l'information est versionnée et à chaque changement, les versions précédentes sont archivées.

La politique de sécurité des systèmes d'information entre en vigueur le jour de sa publication. Dans le cadre de cette diffusion, il existe deux cas :

- Engagement de la Direction Générale et politique de sécurité :
    - Cet engagement devant être connu du plus grand nombre d'acteurs, il est diffusé personnellement aux Directeurs et Managers de Silae qui le diffusent à l'ensemble de leurs équipes. De plus, la politique de sécurité est mise à disposition des équipes dans un espace dédié.

- Procédures détaillant l'application des directives de la Politique de Sécurité des Systèmes d'Information :
    - Ces procédures n'ont pas toute vocation à être diffusées largement et leur diffusion est localisée aux Directions ayant besoin d'en connaître le contenu. Par exemple :
        - Les procédures définissant les clauses spécifiques RH ne sont diffusées qu'aux personnes ad-hoc (DRH, Directeurs Métier, etc.)
        - Les procédures définissant les aspects techniques de l'installation d'un pare-feu ne sont diffusées qu'en interne à la Direction du Service Informatique (Intégrateur, Administrateur, etc.)
    - Certaines procédures peuvent être mises à disposition sur l'Intranet sur décision du Responsable de Sécurité des Systèmes d'Information, particulièrement quand elles ont une vocation méthodologique (Intégration de la Sécurité Dans les Projets, etc.)
    - Dans le cadre d'Audits :
        - Les documents peuvent être présentés aux auditeurs et fournis une fois anonymisés en cachant les données confidentielles (Données personnelles, adresses IP des schémas, login, etc.) à condition que l'auditeur souhaite conserver des preuves d'Audit.
    - Ces procédures ne peuvent en aucun cas être fournies à des clients.

4. POLITIQUE GLOBALE DE SECURITE

Le présent Plan d'Assurance Sécurité s'applique :

- Aux environnements d'hébergement externalisés, certifiés ISO 27001, exploités par Silae dans le cadre de ses offres de service ainsi que pour son usage en interne :
    - La liste des datacenters concernés (Hébergement en France ou en Europe)
        - Les datacenters hébergés et infogérés par Orange
        - Les datacenters hébergés et infogérés par Microsoft France
        - Le datacenter hébergé et infogéré par OVH
    - Incluant dans le périmètre de la prestation :
        - Les actifs matériels propriété de l'hébergeur et maintenus par ce dernier
        - Les infrastructures virtuelles (VirtualDataCenter) gérées par Silae
        - Les serveurs virtuels servant d'hôtes pour les applications
- Aux applications métier, bases de données proposées par Silae, classées suivant le RGPD :
    - En tant que responsable de traitement
    - En tant que sous-traitant
- Aux postes de travail personnels
- Aux infrastructures réseau (Datacenters et bureaux)

En ce qui concerne les données, une classification est mise en place afin de définir les conditions de manipulation et la criticité selon les exigences légales.

Les politiques essentielles de sécurité sont les suivantes :

- Patch Management
- Antivirus
- Sauvegardes
- Gestion des traces
- Gestion et maintenance du matériel
- Gestion du réseau
- Contrôle des accès aux données
- Contrôle des accès physiques
- Normes des nouvelles applications
- Normes de développement
- Gestion des incidents
- Capacity Planning

5. PROTECTION DES DONNEES

L'architecture matérielle et logicielle et les procédures d'organisation mises en œuvre par Silae permettent de garantir :

- La confidentialité des données
- L'intégrité des données
- La disponibilité des données

Il n'existe qu'un seul système de management de la sécurité de l'information garantissant confidentialité, intégrité et disponibilité pour toutes les données, qu'elles soient personnelles ou non.

Silae procède à la mise à jour complète des systèmes comprenant :

- Les mises à jour de sécurité
- Les mises à jour d'application (correction des bugs)

Ces mises à jour sont effectuées manuellement après validation sur les serveurs de recette. De manière similaire, elles sont planifiées dans une plage horaire, de préférence en dehors des heures de travail. Certaines mises à jour de sécurité nécessitant un redémarrage des machines, des plages de maintenance dédiées sont prévues, au minimum une fois par semaine.

Tous les postes de travail sont sécurisés par la solution « Bitlocker » qui chiffre le contenu des supports de stockage des postes de travail. Cette sécurisation vise à éviter toute fuite de données compréhensibles en cas de vol ou de tentative d'exploitation d'un support de stockage comme un disque dur.

Le télétravail obéit aux mêmes règles de sécurité que sur les sites Silae.

- Tous les postes de travail des collaborateurs sont équipés d'un antivirus qui se met à jour automatiquement et quotidiennement. Des analyses automatiques régulières sont également effectuées sur ces postes. En cas de détection d'un fichier malveillant, le département sécurité est automatiquement alerté, et les actions suivantes sont immédiatement mises en œuvre :
    - Tentative de réparation du fichier
    - Tentative de mise en quarantaine du fichier
    - Tentative de suppression du fichier

En cas d'échec des actions automatiques suscitées, l'équipe sécurité prend en charge le nettoyage du poste.

Les serveurs de Silae sont équipés d'un système anti-intrusion bénéficiant de mises à jour quotidiennes. Le traitement des fichiers malveillants suit une procédure identique à celle appliquée aux postes de travail individuels. Les alertes sont transmises à l'équipe sécurité et consignées dans le système de gestion des incidents techniques.

6. SUPPRESSION SECURISEE DES DONNEES

Silae a mis en place des procédures rigoureuses pour la garantir la destruction sécurisée des données collectées durant l'utilisation de ses produits et services, lorsque leur stockage n'est plus nécessaire ou à la fin de la relation contractuelle. Les matériels de stockage ou les services dédiés à l'hébergement des données en fin de vie sont décommissionnés selon un processus formel géré par l'hébergeur certifié ISO 27001 qui en est propriétaire.

Le matériel utilisé par les collaborateurs de Silae fait également l'objet de procédures rigoureuses d'effacement sécurisé des données, grâce à l'utilisation d'une solution certifiée conforme aux standards internationaux en matière de destruction des données. L'élimination des appareils en fin de vie s'effectue dans le respect de la politique environnementale de l'entreprise, garantissant une gestion responsable et durable de ces équipements. Par ailleurs, des traces détaillées sont systématiquement collectées pour chaque opération de destruction de données et d'élimination de matériel.

7. GESTION DES ACCES INTERNES

Afin de garantir la conformité avec les exigences de contrôle d'accès, Silae utilise une application dédiée à la gestion des actifs (GLPI), couvrant à la fois les machines et les comptes utilisateurs. Cette solution centralisée assure une gestion efficace des droits d'accès, en appliquant rigoureusement les principes de « moindre privilège » et de « besoin d'en connaître ».

L'application est accessible exclusivement aux équipes IT et sécurité. Par ailleurs, une application dédiée est mise à disposition du service RH et des managers responsables, leur

permettant de mettre à jour les informations relatives au cycle de vie des comptes. Cette fonctionnalité facilite la création, la modification et la suppression des comptes, dans le respect des processus formalisés et documentés.

Les droits d'accès sont accordés de manière strictement contrôlée, et les journaux des actions sont archivés afin de garantir une traçabilité optimale. En outre, l'utilisation de comptes partagés ou génériques est formellement interdite. Ce dispositif renforce à la fois la sécurité et la transparence dans la gestion des accès aux systèmes sensibles.

8. POLITIQUE DE COMPTES ET DE MOTS DE PASSE

Les comptes permettant l'authentification au système d'information de Silae sont uniquement des comptes individuels répondant au principe de moindre privilège. Ceux-ci sont systématiquement liés à un utilisateur ou un administrateur et sont nominatifs. Une revue de comptes régulière est menée afin de s'assurer :

- Qu'aucun compte n'est inactif depuis plus de 90 jours.
- Que les droits liés aux comptes sont cohérents avec les besoins.
- Que le niveau de sécurité des comptes et bien cohérent avec la criticité de ceux-ci.

Dans le cadre de la politique de mots de passe de Silae , les règles de constitution de ces mots de passe sont les suivantes :

Compte Utilisateur :

- Doit être composé d'une longueur supérieure ou égale à 12 caractères
- Doit contenir au moins deux caractères spéciaux
- Doit contenir au moins un chiffre
- Doit comporter les lettres minuscules ET majuscules
- Doit être automatiquement bloqué après 3 essais infructueux
- Ne doit pas être composé d'aucun terme propre à l'utilisateur ou à l'entreprise
- Ne doit pas être enregistré en clair (au sein d'un fichier), ni pouvoir être déduit par une fonction quelconque ou d'une chaîne de caractères
- Doit faire l'objet d'un contrôle automatique de robustesse

Ou

- Doit obtenir un score supérieur ou égal à 71 au calcul d'entropie disponible ici

Compte Administrateur :

- Doit être composé d'une longueur supérieure ou égale à 15 caractères
- Doit contenir au moins deux caractères spéciaux
- Doit contenir au moins un chiffre
- Doit comporter les lettres minuscules ET majuscules
- Doit avoir obligatoirement une durée de vie maximale de 180 jours
- Doit être automatiquement bloqué après 3 essais infructueux

- Ne doit pas être composé d'aucun terme propre à l'utilisateur ou à l'entreprise
- Ne doit pas être enregistré en clair (au sein d'un fichier), ni pouvoir être déduit par une fonction quelconque ou d'une chaîne de caractères
- Doit être différent des 10 derniers mots de passe
- Doit faire l'objet d'un contrôle automatique de robustesse
- Doit être associé à un système d'authentification multifacteurs

Ou

- Doit obtenir un score de 89 au calcul d'entropie disponible ici

Au sein de Silae, un gestionnaire de mots de passe de confiance est obligatoirement utilisé pour la génération et la conservation des mots de passe.

Chaque utilisateur ou administrateur est responsable de la sécurité de ses authentifiants, de leur utilisation, ainsi que du signalement d'incidents en cas de compromission.

Silae garantit que l'accès des utilisateurs aux systèmes et applications est sécurisé conformément aux meilleures pratiques d'authentification et de gestion des mots de passe. Les journaux d'accès, ou logs d'accès, sont conservés dans le respect du cycle de vie défini dans la politique de sécurité de l'entreprise. Ces logs d'accès sont conservés pour garantir la disponibilité des données d'audit et pour fournir un support essentiel lors d'éventuelles investigations ou analyse liées à des incidents de sécurité. Ces logs permettent d'identifier les tentatives de connexion, leurs résultats, et les actions menées sur les données. Ce mécanisme renforce la capacité à détecter, analyser et remédier rapidement aux menaces potentielles, tout en assurant une traçabilité complète.

9. VEILLE SECURITE

Le département sécurité réalise une veille quotidienne pour identifier les vulnérabilités existantes et garantir la mise en œuvre rapide d'actions permettant de réduire ou d'éviter les risques associés.

Afin d'assurer cette veille, Silae s'appuie sur les sources suivantes :

- CrowdStrike Falcon Complete et Microsoft Defender alertant sur les vulnérabilités identifiées à l'échelle mondiale et propre à Silae
- Solution de sensibilisation à la sécurité de l'information alertant sur les fuites d'informations confidentielles connues au sein des entreprises partout dans le monde
- Différentes communautés de Cyber sécurité Françaises, comme le CESIN
- Organismes d'état (ANSSI, CISA, CERT-FR, etc.)
- Réseaux sociaux dédiés
- Blogs et sites internet dédiés à la sécurité des systèmes d'information
- Remontées internes et externes

En cas de vulnérabilité identifiée susceptible de représenter un risque pour le système d'information de Silae, une analyse est effectuée et des actions sont mises en œuvre pour sécuriser le système. Les outils de communication internes de Silae sont mobilisés pour informer les différents intervenants concernés. La direction de Silae s'engage activement dans le suivi et la résolution de ces vulnérabilités et participe directement aux décisions liées à leur gestion.

10. SURVEILLANCE DE LA DISPONIBILITE DES SERVICES

Silae déploie des moyens matériels et humains très importants afin de garantir une disponibilité maximale de ses produits et services pour ses utilisateurs. Pour assurer cette disponibilité, l'entreprise s'appuie exclusivement sur des hébergeurs certifiés ISO 27001, reconnus comme des leaders dans leur secteur d'activité.

Les ressources dédiées au fonctionnement des produits et services sont conçues pour être élastiques, s'ajustant automatiquement à la charge d'usage afin de prévenir toute interruption ou dégradation de la qualité des services. Selon les produits, des mécanismes de Plan de Continuité d'Activité (PCA) ou de Plan de Reprise d'Activité (PRA) peuvent être mis en place. Lorsqu'ils sont appliqués, ces mécanismes sont documentés dans les Plans d'Assurance Sécurité Annexes.

11. GESTION DES VULNERABILITES

Lorsqu'un scan de vulnérabilités ou un test d'intrusion révèle des vulnérabilités dans un produit ou service de Silae, celles-ci sont immédiatement intégrées dans le processus de gestion des vulnérabilités.

Dans un premier temps, les vulnérabilités identifiées sont classées selon leur criticité à l'aide du CVSS (Common Vulnerability Scoring System), qui attribue une note sur une échelle de 0 à 10. Une note de 0 indique l'absence de vulnérabilité, tandis qu'une note de 10 correspond à une vulnérabilité extrêmement critique. Ce score est calculé en fonction de plusieurs critères, notamment l'impact sur la confidentialité, l'intégrité, la disponibilité, ainsi que la facilité d'exploitation de la faille.

Afin d'assister les équipes sécurité dans ce calcul, l'outil : Common Vulnerability Scoring System Version 3.1 Calculator mis à disposition par first.org est utilisé.

Ce calcul permet un classement des vulnérabilités comme suit :

Score CVSS minimum	Score CVSS maximum	Correspondance
0	3.9	Faible (Low)
4	6.9	Modérée (Medium)
7	8.9	Élevée (High)
9	10	Critique (Critical)

Afin de s'assurer du traitement rapide des vulnérabilités identifiées, des délais maximums de lancement de remédiation ont été déterminés comme suit :

Criticité	Durée de remédiation appliquée (Maximum)
Faible (Low)	1 trimestre
Modérée (Medium)	1 mois
Élevée (High)	1 semaine
Critique (Critical)	24h

12. GESTION DES INCIDENTS DE SECURITE

Un incident de sécurité des systèmes d'information désigne un événement, potentiel ou avéré, indésirable et/ou inattendu, susceptible d'affecter gravement la sécurité des systèmes d'information. Cet impact peut concerner la disponibilité, la confidentialité, l'intégrité ou la traçabilité des données, ainsi que la protection de la vie privée.

Tout incident de sécurité observé ou suspecté est signalé à l'équipe Sécurité par les collaborateurs ou les prestataires. Cet incident entre ensuite dans le plan de gestion des risques dans lequel il est catégorisé et traité. Une revue mensuelle des incidents de sécurité est menée par l'équipe Sécurité qui dégage et globalise des plans d'action correctifs pérennes.

En cas d'incident ayant un impact sur les données de nos partenaires, ceux-ci sont alertés dans un délai maximum de 72 heures par leur point de contact dédié au sein de Silae et une cellule de crise est mise en place avec le partenaire afin de garantir la communication en temps réel des informations liées à l'incident. Le DPO de Silae est immédiatement impliqué dans tous les échanges sur le sujet. À l'issue de la gestion de crise, un compte rendu d'incident peut être fourni au partenaire à sa demande.

La cellule de crise externe mise en place est distincte de la cellule de crise interne à Silae, à laquelle participent tous les intervenants concernés par l'incident. Ces deux cellules sont cloisonnées afin de garantir qu'aucune information confidentielle de Silae ne soit communiquée à des tiers.

13. BUSINESS CONTINUITY PLANNING

Le Business Continuity Planning interne de Silae est défini comme suit :

13.1 Plan de risque pandémique ou urgence santé interne

Silae dispose d'un système global de gestion de la santé et de la sécurité développé pour se conformer aux exigences réglementaires nationales et aux lignes directrices en cas de crise nationale ou internationale.

Par ailleurs, le système de gestion de la santé et de la sécurité est conçu pour prévenir les accidents et les blessures tout en garantissant le respect de l'ensemble des exigences réglementaires applicables sur les lieux de travail de tous les sites. Ce système s'applique à l'ensemble des sites de Silae, chacun étant tenu de se conformer aux exigences et réglementations pertinentes qui le concernent.

13.2 Programme de continuité SI interne

Silae dispose d'un programme global de continuité des activités géré par une équipe dédiée. Ce programme comprend des plans de continuité des activités (PCA) créés pour les fonctions critiques de l'entreprise (messagerie, partages, applications, etc.) Les PCA décrivent les procédures de restauration des processus essentiels en cas d'indisponibilité des ressources, y compris la perte de bâtiments, de technologies, de ressources humaines, de fournisseurs tiers ou d'équipements.

Chaque année, les Plans de Continuité d'Activité (PCA) sont examinés et testés avec des participants spécifiquement désignés pour chaque plan. Ces exercices incluent une orientation ainsi que des scénarios adaptés aux équipes et/ou aux produits concernés. Ils sont réalisés annuellement afin de renforcer et de maintenir la résilience organisationnelle pour l'ensemble des équipes et des produits. Chaque PCA est supervisé par la direction générale pour les principaux domaines fonctionnels de Silae et bénéficie du soutien de la direction exécutive. Les équipes individuelles sont responsables de l'élaboration et de la mise à jour de leurs plans respectifs, de la formation du personnel sur leurs rôles et responsabilités, ainsi que de la mise à jour régulière de ces plans.

Silae procède également à une analyse annuelle de l'impact sur les activités (Business Impact Analysis / BIA) afin d'identifier les conséquences opérationnelles et financières de toute perturbation imprévue des activités de Silae. Le BIA est associé à un processus décrivant les responsables de processus, les dirigeants et les autres employés concernés de Silae. Le BIA inclut les impacts qualitatifs et quantitatifs possibles, les applications et les fournisseurs critiques, les lieux et toute information susceptible d'aider à identifier les risques de reprise ou les lacunes nécessitant des mesures d'atténuation.

13.3 Programme de continuité des sites de production

Les solutions Silae sont hébergées dans des centres de données tiers. Chaque produit ou service proposé par Silae dispose d'un plan de reprise ou de continuité d'activité développé de manière indépendante des autres produits.

Silae met systématiquement en œuvre, au minimum, un plan de reprise d'activité (PRA) pour ses produits. Dans certains cas, un plan de continuité d'activité (PCA) peut également être en vigueur. Lorsque c'est le cas, ce plan est documenté dans l'annexe de sécurité associée au produit concerné.

Silae maintient systématiquement des environnements distincts pour la production, le développement et les tests. Chaque centre de données exploite des architectures (équipements et services) conçus pour supporter la charge tout en garantissant les plus hauts niveaux de performance et de disponibilité. Ces architectures, associées à l'utilisation de ces centres de données, minimise les risques liés aux points de défaillance uniques.

Silae utilise des technologies de réplication fournies par des fournisseurs tiers pour optimiser la précision et l'intégrité de la réplication entre les systèmes de stockage primaires et secondaires. Ces outils logiciels de réplication sont des produits éprouvés, largement utilisés dans l'industrie et reconnus pour leur fiabilité. Des tests réguliers de sauvegarde et d'enregistrement sont effectués pour évaluer le fonctionnement du centre de données. Toutes les données stockées dans les centres de données sont cryptées au repos à l'aide du cryptage AES-256.

Les centres de données sont dotés de dispositifs de sécurité physique, notamment des caméras, une surveillance intérieure et extérieure, des agents de sécurité, ainsi que des badges d'accès. De plus, des installations dédiées à la protection des données sont déployées, telles que des unités d'alimentation électrique, des détecteurs de chaleur, de fumée et d'incendie, ainsi que des dispositifs d'extinction d'incendie.

13.4 Effectifs en cas de catastrophe

Les collaborateurs de Silae sont répartis sur différents sites en France ou opèrent en télétravail. En cas d'indisponibilité d'un site, ils peuvent être mobilisés pour contribuer au rétablissement de ce site, être temporairement transférés vers un autre site disponible ou poursuivre leurs activités en télétravail.

L'ensemble des collaborateurs de l'entreprise dispose des moyens nécessaires pour accomplir leurs missions depuis n'importe quelle localisation, dans des conditions de sécurité optimales. Ces mesures incluent notamment l'usage d'accès VPN sécurisés, des services d'authentification multi-facteurs (MFA) et une solution SaaS dédiée au partage sécurisé des mots de passe.

14. POLITIQUE DE TESTS D'INTRUSION (PENTESTS)

14.1 Tests commandités par Silae

Pour garantir la sécurité des solutions proposées et des données de ses utilisateurs, Silae met en œuvre un programme annuel de tests d'intrusion couvrant l'ensemble de ses produits. Ce programme inclut un test initial annuel ainsi qu'un contre-audit en cas de

découverte de vulnérabilités lors du premier test. Ces tests sont réalisés par des organismes externes spécialisés, sélectionnés par Silae et conformes aux exigences de sécurité définies par l'ANSSI.

En cas de découverte de vulnérabilités, un plan d'actions correctives est élaboré en collaboration entre le département sécurité et les équipes techniques, en s'appuyant sur les recommandations de l'organisme auditeur.

14.1 Partage des documents d'audit commandités par Silae

Les attestations des tests d'intrusion, mentionnant l'organisme ayant réalisé le test ainsi que leur date, peuvent être librement partagées avec les partenaires sur demande.

En revanche, les rapports des tests d'intrusion ne sont en aucun cas communiqués aux partenaires ou à leurs clients. Le détail des vulnérabilités reste strictement confidentiel, car il constitue une information hautement sensible susceptible d'être exploitée par des attaquants externes.

Le partage des synthèses managériales est limité aux partenaires TOP.

Le partage sera réalisé après la signature d'un NDA (Non Disclosure Agreement/Accord de non-divulgation) entre Silae et le partenaire pour chaque audit.

Après la signature du NDA, les éléments suivant seront communiqués :

- Partage de la synthèse du test et de la notation sans aucun détail sur les vulnérabilités.
- Partage de la synthèse du contre audit le cas échéant (si contre audit réalisé) sans aucun détail sur les vulnérabilités ou les corrections effectuées.
- Les documents seront expurgés (biffés) afin de ne pas exposer d'informations sensibles pour Silae, telles que les détails techniques confidentiels, les coordonnées des auditeurs, ainsi que les comptes ou ressources utilisés pour réaliser l'audit, etc.

14.2 Tests commandités par les partenaires

Afin d'être en mesure de réaliser un test d'intrusion, le partenaire doit :

- Faire partie des partenaires TOP de Silae.
- Avoir eu accès et avoir consulté le présent document et les différentes annexes disponibles.

Si une de ces conditions n'est pas remplie, alors la demande de réalisation de test d'intrusion sera refusée, dans le cas contraire, les étapes suivantes doivent être suivies :

- Le partenaire doit envoyer sa demande à son point de contact dédié au sein de Silae comprenant les règles d'engagement, la proposition de date et de durée de l'audit.
- Les différents départements de Silae concernés par le test d'intrusion (Sécurité, produit, engineering, etc.) valident ou non la faisabilité de la demande, ou formulent des demandes de modification de celle-ci.

En cas de validation de la part de Silae, les règles suivantes doivent être appliquées pour l'audit :

- Le programme d'audit doit être envoyé à Silae et validé au moins deux semaines avant le lancement.
- Une spécification écrite de l'étendue de l'audit doit être convenue entre Silae et le partenaire, couvrant l'objectif, l'étendue et les règles d'engagement de l'audit.
- Aucun employé de Silae ne sera chargé de répondre aux questions de l'auditeur pendant l'audit ou de lui apporter un soutien quelconque.
- Les comptes déjà à disposition du partenaire seront utilisés pour mener l'audit.
- Silae ne pourra être tenue responsable en cas d'impact sur la disponibilité, la confidentialité ou l'intégrité des données du partenaire suite aux actions de l'auditeur.
- À la fin de l'audit, un rapport d'audit doit être envoyé à Silae. Ce rapport d'audit doit être utilisable et partageable par Silae de quelque manière que ce soit.
- En cas de constatations de l'auditeur, un plan d'action correctif initial peut être élaboré en concertation avec Silae et le service de sécurité. Toutefois, ce plan ne sera ni transmis au partenaire ni à l'auditeur. Le traitement des vulnérabilités s'effectue conformément aux règles décrites dans la section dédiée du présent document.
- Silae doit approuver formellement le plan d'action avant que les équipes impliquées puissent commencer les actions.

15. POLITIQUE DE SCANS DE VULNERABILITE

En complément des tests d'intrusion annuels commandités par Silae, des scans de vulnérabilités automatisés sont régulièrement effectués sur le système d'information. En cas de détection de vulnérabilités, la procédure de correction appliquée est identique à celle mise en œuvre dans le cadre des tests d'intrusion.

16. GESTION DU CHANGEMENT

En cas de changement susceptible d'avoir un impact sur la sécurité de l'information, le département Sécurité de Silae est systématiquement impliqué dans le projet concerné dès son lancement, avec au minimum un rôle de consultant. Si le chef de projet n'est pas certain de l'existence ou non d'un impact sur la sécurité de l'information, il doit consulter le

département Sécurité pour une analyse et un arbitrage. Toutes les étapes du projet sont consignées et archivées à titre de référence.

Afin d'assurer un suivi rigoureux des changements, et indépendamment des documents produits par le chef de projet, le département Sécurité établit une charte d'implémentation tout au long du projet, garantissant la traçabilité et facilitant les analyses ultérieures. Chaque étape à venir fait l'objet d'une analyse approfondie par le département Sécurité afin d'identifier d'éventuels nouveaux impacts potentiels.

Durant le déroulé du plan d'action lié au projet, des tests sont conduits dans un environnement distinct de ceux de production ne comportant pas de données client ou confidentielles.

Une fois la mise en production réalisée, un audit post-changement est conduit par le responsable du département sécurité et un chargé de sécurité des systèmes d'information, en collaboration avec le chef de projet, afin d'évaluer l'impact final du changement. Un rapport d'audit confidentiel est alors produit et partagé avec la direction.

17. PROTECTION DES POSTES DE TRAVAIL

Les postes de travail des employés de Silae, quel que soit leur niveau d'accès, font l'objet de mesures de sécurité renforcées afin d'éviter toute compromission du système d'information. Les mesures suivantes sont appliquées :

- En cas de non-utilisation d'un poste de travail, celui-ci est verrouillé par son utilisateur dès qu'il le quitte. Si l'utilisateur ne verrouille pas lui-même le poste de travail, un verrouillage automatique est déclenché après 10 minutes.
- Un filtrage web, basé sur une whitelist, est en place afin de limiter les risques de compromission.
- Les utilisateurs ne sont pas administrateur de leurs postes et effectuent des requêtes au travers d'un outil dédié lorsqu'une modification leur semble nécessaire. Cette requête est alors analysée par le département IT qui peut être amené à consulter le département sécurité et qui décide si la requête peut être autorisée.
- Les applications que les utilisateurs peuvent installer sur leurs postes de travail sont disponibles sur une boutique d'application interne à Silae, régulièrement mise à jour en fonction des évolutions métier.
- Tous les disques des postes de travail de Silae sont chiffrés.
- Tous les postes utilisateurs sont scannés par les solutions Microsoft Defender et CrowdStrike, mis à jour sur une base journalière, qui envoient des alertes automatiques au SOC Managé CrowdStrike et au département sécurité de Silae quand cela est nécessaire.
- Les employés de Silae ne sont pas autorisés à utiliser leurs appareils personnels (BYOD) dans le cadre de leurs missions.
- Un SOC managé CrowdStrike est déployé afin de prévenir, contenir et remédier aux menaces Cyber. Nos services de DFIR (Digital Forensics and Incident Response) sont également fournis par CrowdStrike.

Pour le cas spécifique de l'utilisation de supports amovibles, la politique de sécurité des systèmes d'information de SIlae interdit strictement l'utilisation de matériel personnel de ce type. Les ports USB des machines des utilisateurs sont désactivés par défaut afin de limiter les risques liés à l'utilisation non autorisée de médias amovibles. Toute exception à cette règle nécessite une demande formelle de dérogation, qui est soumise à l'examen et à la validation de l'équipe Sécurité pour mise en œuvre par l'équipe IT, conformément au processus de gestion des dérogations. Dans les rares cas où un usage temporaire est autorisé, un chiffrement des données est obligatoire avec copie de la clé fournie à l'équipe IT, conformément à la politique d'usage du chiffrement. Ces mesures renforcent la sécurité des données et minimisent les risques associés aux dispositifs de stockage amovibles.

18. RELATION AVEC L'ISO 27001

La norme ISO 27001 est une norme internationale de sécurité des systèmes d'information dont le nom complet est « Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences » qui est aujourd'hui une des références majeures dans le domaine.

Les prestataires employés par Silae pour héberger les solutions et les données liées à celles-ci sont tous certifiés ISO 27001.

Silae, dans le cadre de son engagement à sécuriser les données de ses clients, base l'intégralité de ses procédures et de son corpus documentaire sur les requis de la norme et de son annexe A. Au sein du département sécurité de Silae, plusieurs membres de l'équipe ont obtenu des certifications ISO 27001, que ce soit en tant que « lead implementor » ou « provisional auditor » leur permettant de veiller au respect des requis.

Silae est actuellement engagée dans une démarche d'obtention de la certification ISO 27001.

19. GESTION ET FORMATION DU PERSONNEL

Les procédures de recrutement de Silae sont conçues pour garantir, dès l'embauche, la sécurité des systèmes d'information. Ainsi, dès les premières étapes du processus de recrutement, des vérifications d'antécédents sont effectuées afin d'exclure les candidats susceptibles de représenter une menace pour la sécurité des données sensibles gérées par Silae.

Lors de l'arrivée d'un employé chez Silae, des identifiants personnels et uniques sont créés pour lui permettre d'accéder exclusivement aux ressources et données nécessaires à l'exécution de ses missions. En cas de départ de l'entreprise, ces accès sont révoqués dans un délai maximum de deux jours ouvrés suivant la date effective de départ.

Afin de maintenir le personnel engagé et compétent sur le sujet de la sécurité des systèmes d'information, Silae a mis en place un programme annuel de sensibilisation et de formation

fonctionnant sur la base de modules dédiés à des sujets définis. Les modules portent sur des sujets variés comme le phishing, la gestion des mots de passe, les différents types de fraude, les malwares, le privacy by design, etc. Afin de maintenir la sensibilisation sur la confidentialité des données, une solution de e-learning est également déployée sur ce sujet, permettant à Silae de s'assurer de la vigilance des collaborateurs sur la durée.

Le suivi de ces modules de formation est obligatoire pour l'ensemble du personnel et un suivi mensuel de leur complétion est réalisé par le département sécurité. En cas de non suivi du programme de sensibilisation, le départements sécurité entre en contact avec le manager de l'employé afin d'effectuer les rappels nécessaires. La direction est engagée dans ce suivi et réalise des communications régulières en ce sens.

Dans le cadre de ce programme de sensibilisation, des campagnes mensuelles de phishing sont organisées auprès des employés de Silae. Ces campagnes consistent à envoyer des emails imitant ceux d'entreprises de confiance ou de collaborateurs internes, afin d'identifier les besoins supplémentaires en formation. Lorsqu'un employé échoue à un exercice de phishing, il est contacté par le département Sécurité, qui lui transmet les bonnes pratiques à adopter en la matière. Par ailleurs, l'analyse des échecs permet d'évaluer le risque potentiel de fuite de données lié à ces incidents ainsi que la robustesse des mots de passe fournis par les collaborateurs lors des exercices.

Les développeurs et les équipes techniques de Silae adoptent des pratiques d'ingénierie et de codage sécurisées en suivant un cycle de développement sécurisé (SDLC) aligné sur les standards de l'industrie. Ces pratiques comprennent des étapes clairement définies pour identifier et gérer les risques de sécurité tout au long du processus de développement, telles que des revues de code, manuelles ou automatisées, à l'aide d'outils comme SonarQube, ainsi que des validations de conformité. Ces mesures garantissent l'intégration proactive de la sécurité à chaque phase du cycle de vie des systèmes et applications.

20. PRISE EN CHARGE DES QUESTIONS RELATIVES A LA SECURITE DE L'INFORMATION

Afin d'accompagner au mieux ses partenaires dans le cadre des questions relatives à la sécurité de l'information, Silae a déployé une procédure interne sur le sujet. Lorsqu'un partenaire à une ou plusieurs questions relatives à la sécurité de l'information, celui-ci doit les faire remonter à son point de contact privilégié qui suivra la procédure interne de réponses aux questions en les transmettant au service compétent.

Afin de garantir au mieux la réponse à ces questions, certaines conditions doivent être remplies :

- Le partenaire a consulté le présent document et ses annexes afin de vérifier si la réponse à sa question n'y est pas déjà présente.
- Le partenaire s'est référé aux réponses aux questions qu'il avait déjà obtenues afin de s'assurer que la réponse n'avait pas déjà été apportée.

- Les questions doivent porter sur la sécurité des systèmes d'information ou la protection des données.

Une fois les questions reçues, le service compétent les consultera et y apportera les réponses avant de les retransmettre au point de contact dédié au partenaire. Cependant, certaines questions portant sur des procédures, documents ou informations internes confidentielles pourront se voir opposer un refus de réponse. La décision de répondre ou non à une question portant sur la sécurité de l'information est uniquement à la discrétion de Silae.

21. GESTION DES DEROGATIONS

Silae peut, si nécessaire, accorder des dérogations à sa politique de sécurité des systèmes d'information. Pour qu'une dérogation soit validée, il est impératif de suivre une procédure interne préalablement définie.

« Une dérogation à la politique de sécurité des systèmes d'information est nécessaire quand la politique actuelle à un impact négatif sur la capacité de travail d'un employé ou d'un département. Une dérogation à la politique de sécurité des systèmes d'information matérialise une autorisation délivrée à un employé de Silae ou un département à ne pas suivre tout ou partie d'une procédure de sécurité. »

Afin qu'une dérogation soit étudiée, une demande formelle doit être envoyée au département sécurité de Silae comprenant les informations nécessaires à l'étude de celle-ci. Le département sécurité analyse alors la demande afin d'identifier :

- Les éventuelles vulnérabilités qu'une telle dérogation pourrait entraîner.
- Le risque associé.
- Le niveau d'acceptabilité de ce risque.
- La durée d'acceptabilité de ce risque.
- Les actions qui pourraient être réalisées pour réduire ce risque en cas d'acceptation.
- Le responsable du risque.
- La capacité du responsable du risque à accepter ce risque.

En cas d'acceptation de la dérogation, celle-ci est consignée et archivée dans un emplacement dédié et ajoutée au registre des risques. Celle-ci sera alors prise en compte lors des différentes revues et analyses du registre des risques.

Lors du suivi de la procédure dédiée aux dérogations à la politique de sécurité des systèmes d'information, les principes généraux suivants s'appliquent :

- Une acceptation de dérogation ne peut en aucun cas être définitive et requiert a minima une date de début et une date de fin.
- Certaines dérogations peuvent éventuellement être renouvelées à la date de fin de validité uniquement si ceci avait été abordé lors du processus d'acceptation.

- Si une dérogation a été refusée, cette décision en peut changer sans une nouvelle demande formalisée.
- Une dérogation ne peut exister sans la signature des deux parties (demandeur et département sécurité.)
- Le département sécurité se réserve le droit de révoquer une dérogation à la politique de sécurité des systèmes d'information si une vulnérabilité sérieuse associée à un nouveau risque apparaît durant la période de validité de celle-ci.

Une fois la période de validité de la dérogation expirée, et uniquement si la possibilité d'un renouvellement de celle-ci avait été abordée lors du processus d'acceptation, la dérogation peut être renouvelée si les règles suivantes sont respectées :

- Une demande formelle de renouvellement a été envoyée au département sécurité par le demandeur.
- Une nouvelle analyse du risque a été réalisée par le département sécurité.
- Une nouvelle attestation d'acceptation signée par les deux parties a été transmise au demandeur.

22. CLASSIFICATION DES INFORMATIONS

Silae a défini plusieurs niveaux de classification des informations associés à des règles de diffusion.

Le premier niveau de classification défini par Silae est le niveau « Public ». Ce niveau de classification permet un partage de l'information sans restriction.

Le deuxième niveau de classification défini par Silae est le niveau « Restricted / Restreint ». Ce niveau de classification permet un partage uniquement avec l'accord formel des parties prenantes associées à l'information.

Le troisième niveau de classification défini par Silae est le niveau « Confidential / Confidentiel ». Ce niveau de classification ne permet le partage de l'information qu'avec l'accord formel des parties prenantes associées à l'information et la signature d'une NDA de la part du receveur.

Le quatrième et dernier niveau de classification défini par Silae est le niveau « Secret ». Ce niveau de classification ne permet pas le partage de l'information en dehors des parties prenantes associées à celle-ci.

Une déclassification peut-être nécessaire pour une information spécifique si une des conditions suivantes s'applique :

- Le contenu d'un document a été mis à jour, le sortant des règles de classification actuellement appliquées.
- Un document doit être partagé avec une audience plus large pour des raisons exceptionnelles.

- Une loi ou une réglementation officielle a été mise à jour ou modifiée, menant à une modification des règles de classification.

Afin de déclassifier un document, une procédure interne est définie, impliquant la formalisation de la demande et de sa justification. Cette demande passe par un processus de validation multiple impliquant notamment les parties prenantes liées à l'information et la direction de Silae avant de pouvoir être déclassifiée. L'intégralité des étapes de ce processus est consignée pour en garantir la traçabilité.

23. SECURITE DES COMMUNICATIONS

Afin de sécuriser la transmission de données, plusieurs mesures techniques sont mises en place.

En premier lieu, les données sont systématiquement chiffrées en transit au travers de l'utilisation du protocole HTTPS pour toutes les communications réalisées au sein du système d'information de Silae.

Les communications par email, quant à elles, sont sécurisées par les protocoles de chiffrement de Outlook qui est le seul client email utilisé par l'ensemble des employés de Silae. Une solution d'analyse antispam a également été ajoutée à la configuration du client email afin d'améliorer la sécurité de ce dernier.

Enfin, le partage de documents peut également se faire au travers de l'utilisation de solutions de confiance développées par Silae comme eDoc Sign ou eDoc Perso.

L'accès à distance au système d'information de Silae par les employés de l'entreprise ou les prestataires externes sélectionnés par celle-ci est protégé par l'utilisation de comptes individuels renforcés par l'authentification multifacteur et le SSO Microsoft. De plus, les équipements non maîtrisés par Silae ne permettent pas l'accès au système d'information.

24. ANALYSE DE RISQUES

Silae procède à des analyses des risques régulières afin de conserver une connaissance et une compréhension accrue des risques Cyber pesant sur l'entreprise. Pour ce faire, chaque vulnérabilité identifiée et le risque associé sont consignés dans un registre des risques mis à disposition de la direction, du DPO et du département sécurité. Ce registre fait également état de l'évaluation des risques et du suivi des actions correctives.

Dans le cadre de cette analyse de risques, plusieurs instances sont mises en place. La première consiste en une revue mensuelle du registre des risques entre le DPO et le département sécurité. Durant cette revue, un état des lieux des avancées des actions liées aux risques est réalisé, et un tour de table permet d'identifier d'éventuelles vulnérabilités qui n'auraient pas été consignées dans le registre. La seconde instance consiste en une revue trimestrielle avec la direction, permettant de transmettre les dernières découvertes

et d'analyser les différents risques afin d'adapter la stratégie sécurité. Ces revues concernent l'intégralité des risques liés à Silae, que ce soit au niveau de l'entreprise ou des solutions proposées, des tiers et des employés.

Mensuellement, des KPIs sont calculés et analysés, permettant d'élaborer une note de risque Global pour l'entreprise, un suivi des risques résolus et du volume d'entrées dans le registre des risques.

Dans le cadre des traitements pouvant impliquer la collecte de données sensibles, SIlae procède également à des analyses d'impact sur la vie privée conformément au RGPD.

25. PARTAGE DE LA DOCUMENTATION SECURITE AUX PARTENAIRES

Silae permet le partage de certains documents aux partenaires au travers d'un SharePoint dédié accessible depuis l'externe. Le lien vers ce SharePoint est communiqué aux partenaires par leur point de contact dédié chez Silae.

Dans le cadre du partage de documents non prévus à cet effet, et ce très exceptionnellement, le département sécurité de Silae peut être amené à « caviarder » certains documents, et à les partager sous forme de fichier non modifiable et non sélectionnable en apposant un watermark indiquant le nom de l'entreprise ou de la personne receveuse et la date de partage.

Le partage des documents d'audit (Tests d'intrusion/Pentest) est régi par la section dédiée à ce sujet.

26. SECURISATION DES RESEAUX ET DES EQUIPEMENTS

Silae a mis en place des contrôles d'accès renforcés pour les réseaux sans fil, en utilisant des technologies de chiffrement et d'authentification conformes à l'état de l'art, telles que WPA3 et 802.11 EAP, afin de garantir la confidentialité et l'intégrité des communications. De plus, des pare-feu physiques sont mis en place afin de sécuriser les connexions au réseau interne.

Les baies de brassage et serveurs, ainsi que tout le matériel associé, présents au sein des sites de Silae sont situés dans des zones sécurisées pour lesquelles sont appliquées des mesures de sécurisation des accès supplémentaires. Tous les collaborateurs ayant accès à ces zones sont identifiés.

Les connexions aux ressources cloud sont sécurisées grâce à l'application stricte du principe du « moindre privilège », gérées via notre fournisseur d'identité. Ce dernier offre une gestion centralisée des accès et des politiques d'authentification forte pour garantir que seuls les utilisateurs autorisés peuvent accéder aux données. Ces mesures assurent une sécurité robuste pour tous les accès réseau, alignée avec les exigences de protection des données sensibles. Nous effectuons des revues hebdomadaires des topologies réseau et des configurations de stockage afin de garantir la conformité réglementaire et contractuelle, ainsi que l'application stricte des principes du « moindre privilège » et du « besoin d'en connaître ». Ces revues permettent d'identifier et de corriger proactivement toute déviation par rapport aux contrôles de sécurité de l'information convenus. De plus, la direction procède à un examen annuel des contrôles techniques et organisationnels en place pour protéger les données.

27. SECURITE PHYSIQUE

Les sites de Silae n'hébergent aucunes données client quelles qu'elles soient. En effet, toutes les données sont hébergées dans des data centers externes certifiés à minima ISO 27001. La sécurité sur ces sites est alors à la charge des différents hébergeurs.

Concernant les sites de Silae, ceux-ci sont protégés par l'utilisation de badges d'accès, de vidéo surveillance et/ou d'alarmes dont la gestion est effectuée par des prestataires externes spécialisés également en charge des mesures de levée de doute. Les accès font l'objet de logs, stockés sur un serveur sécurisé et pouvant faire l'objet d'analyses en cas de nécessité.

Concernant les zones à accès restreint, l'accès est strictement limité au personnel autorisé et s'accompagne de mesures de sécurité renforcées.

28. GESTION DE LA SECURITE AVEC LES SOUS-TRAITANTS

Afin d'assurer la sécurité de son système d'information, Silae contractualise le suivi de sa politique de sécurité avec ses sous-traitants. Concernant les hébergeurs, ceux-ci étant tous certifiés ISO 27001 et le Système de Management de la sécurité de l'information de Silae étant basé sur les requis de cette norme, la présentation de ces certificats garantie le bon suivi de notre politique de sécurité.

Concernant les autres sous-traitants pouvant être amenés à effectuer des missions sur le système d'information de Silae, les contrats avec ceux-ci sont édités avec a minima une notion d'engagement à respecter la politique de sécurité de l'entreprise et une clause de non-divulgation effective durant toute la durée du contrat et après la clôture de celui-ci.