Politique de Sécurité des Systèmes d'Information
SM 16 601
Ed 8

Confidentialité		
Note	**Confidentialité**	**Niveau (à cocher)**
1	Document public	X
2	Document restreint à la société	
3	Document restreint à un groupe de personnes	
4	Document confidentiel restreint aux personnes concernées	

Suivi des versions				
Date	**Versions**	**Auteur(s)**	**Validé (V) / Approuvé (A) par**	**Motif de la version**
21/01/2016	Ed. 1	SV	Comité de sécurité	Version originale
22/03/2017	Ed. 2	SV	Comité de sécurité	Modification de la règle 9.2.3
28/06/2018	Ed. 3	SV	Comité de sécurité	Ajout de la règle 9.10.6 et du paragraphe 9.16
10/07/2019	Ed. 4	SV	Comité de sécurité	Modification du paragraphe 2, modification de termes, modification de la règle 9.14.4 et modification du paragraphe 9.16
17/07/2020	Ed. 5	SV	Comité de sécurité	Modification du paragraphe 7 et ajout du paragraphe 9.17
25/06/2021	Ed. 6	SV	Comité de sécurité	Correction d'un renvoi au paragraphe 9.12
24/06/2022	Ed. 7	SV	Comité de sécurité	Modification du paragraphe 9.7
23/06/2023	Ed. 8	FGB	Comité de sécurité	Modification aux chapitres 9.5 à 8 ; 9.10 à 11 et 9.17

Sommaire

1 - Objet

Ce document constitue le référentiel, aussi appelé « Politique de sécurité des Systèmes d'Information » de la société Invoke. Il est construit à partir du « guide pour l'élaboration d'une politique de Sécurité des Systèmes d'Information » de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Ce document est conçu et formalisé par le Comité de Sécurité de la société, instauré pour prendre en charge les diverses problématiques de sécurité liées à l'activité d'Invoke et de ses filiales. Il reflète la volonté et les exigences en matière de sécurité de la société Invoke mises en œuvre pour la protection de son Système d'Information, tant au niveau de ses biens (données, informations, serveurs, équipements réseau, …) que du fonctionnement global de l'ensemble.

2 - Contexte

La société Invoke, de par son activité d'éditeur de logiciels, dispose d'un certain nombre d'informations sensibles qu'il convient de protéger afin de préserver ses activités ainsi que son image.

Ces données recouvrent :

- Le patrimoine intellectuel, composé de toutes les informations nécessaires au maintien et au développement de son activité, incluant le code source de ses logiciels (déposés et/ou brevetés), les processus de développement, la documentation, et d'une manière plus générale, le savoir-faire développé depuis plusieurs années.
- Les données des clients pour lesquels Invoke assure un Service SaaS « Software As A Service » ou des prestations de type Services Professionnels et/ou Support (assistance téléphonique).
- Les informations relatives à ses clients, ses partenaires ou tout tiers avec lequel la société a des relations et dont l'altération ou la divulgation pourrait porter atteinte à l'image ou aux activités de la société.
- Les informations relatives aux personnes, tels que les dossiers administratifs ou d'appréciation, dont la divulgation constituerait une violation de la vie privée.
- Les données et informations relatives à ses salariés, intérimaires, stagiaires, alternants ci-après Collaborateurs et dont l'altération ou la divulgation pourrait porter atteinte à l'image ou aux activités de la société.

- La protection de l'ensemble de ces données nécessite la prise en considération d'un contexte organisationnel complexe caractérisé par :
    - La répartition géographique de la société (internationale).
    - L'utilisation de technologies et logiciels hétérogènes offrant des moyens de communication puissants, internes et externes.
    - Les besoins techniques des différentes équipes induisant un grand nombre d'environnements hétérogènes de test ou de support à maintenir.

3 - Orientation stratégique

La stratégie de Sécurité des Systèmes d'Information est séparée entre deux typologies d'informations : les informations de production et les informations de test.

Cette distinction sous-entend que toute donnée de production est considérée comme devant être accessible à un propriétaire qui peut décider ou non de sa publication. A l'inverse, toute donnée de test est considérée comme devant être restreinte à la société, à moins que le propriétaire de cette dernière la qualifie autrement lors de la mise en œuvre des outils ou technologies employés dans ce cadre.

Cette orientation a pour objectif de faciliter la productivité et la communication en évitant une surprotection de l'information lorsque cela n'est pas nécessaire. Cette orientation permet néanmoins de proposer des mécanismes de sécurisation pour toute donnée qui l'exige.

4 - Périmètre

La Politique de Sécurité des Systèmes d'Information s'applique à la société Invoke ainsi qu'à ses filiales. Ce périmètre comprend l'ensemble des moyens humains, techniques et organisationnels en lien avec l'utilisation des données de la société, quelle que soit la forme de ces dernières (électroniques, imprimées, manuscrites, …).

Cette politique concerne l'ensemble des activités et métiers de la société, quels que soient leurs lieux d'implémentation.

Elle s'applique à :

- L'ensemble des personnels autorisés à accéder, utiliser ou traiter, au niveau fonctionnel ou technique, des informations ou des biens des Systèmes d'Information d'Invoke.

- L'ensemble des Collaborateurs et entités d'Invoke.
- L'ensemble des tiers, dès lors qu'ils utilisent les Systèmes d'Information de la société.
- L'ensemble des données d'Invoke, quel qu'en soit le support ou la nature.
- Tous les composants matériels et logiciels des Systèmes d'Information, et en particulier :
    - Les applications, processus de traitement, bases de données et les serveurs qui les hébergent.
    - Les réseaux de communication.
    - Les moyens et environnements techniques de fonctionnement des équipements.
    - Les bâtiments et locaux hébergeant les ressources humaines et les moyens informatiques de la société.

5 - Enjeux de la PSSI

La Sécurité des Systèmes d'Information (SSI) est une composante essentielle de la protection de la société Invoke dans ses intérêts propres ainsi que ceux de ses clients.

Face aux risques encourus, il convient d'identifier ce qui doit être protégé, de quantifier l'enjeu correspondant et d'évaluer, arbitrer et mettre en œuvre les parades adaptées au juste niveau de sécurité retenu. Cela passe prioritairement par la définition et la mise en place d'une « Politique de Sécurité des Systèmes d'Information » (PSSI) prenant en compte les principaux risques identifiés lors de la phase d'analyse des activités métiers :

- Risque d'indisponibilité des informations et des systèmes les traitant (intrusion, vol, destruction, panne, déni de service) qui porterait préjudice aux activités d'Invoke et entrainerait des risques contractuels vis-à-vis de ses clients.
- Risque de divulgation ou de perte de confidentialité qui entrainerait :
    - Pour les données d'Invoke : un risque de perte de compétitivité si des données propres à son savoir-faire intellectuel ou ses stratégies de développement venaient à être divulguées.
    - Pour les données de ses clients : un risque de divulgation d'informations stratégiques ou financières pouvant porter préjudice à leur image ou leur activité.

- Risque d'altération des informations pouvant entrainer une perte de qualité des logiciels ou des prestations fournies. Ce risque peut entrainer également la publication d'états ou déclarations erronés pour les clients hébergés.

6 - Les besoins de sécurité

La sécurité des Systèmes d'Information repose sur quatre critères (DICT) :

- **Disponibilité** : garantir que les éléments considérés (fichiers, messages, applications, services) sont accessibles au moment voulu par les personnes autorisées.
- **Intégrité** : garantir que les éléments considérés (données, messages, …) sont exacts et complets et qu'ils n'ont pas été modifiés.
- **Confidentialité** : garantir que seules les personnes autorisées ont accès aux éléments considérés (applications, fichiers, …).
- **Traçabilité** : garantir que les accès et tentatives d'accès aux informations sont tracés et que ces traces sont conservées et exploitables en temps voulu.

Ces quatre critères sont évalués pour chaque bien le nécessitant et notés sur une échelle de 1 à 4 afin de refléter chaque besoin :

	Disponibilité	**Intégrité**	**Confidentialité**	**Preuve**
1	Non critique	Besoin faible	Donnée publique	Besoin faible
2	< 1 semaine	Besoin moyen	Donnée restreinte à la société	Besoin moyen
3	< 24 heures	Besoin important	Donnée restreinte à un groupe de personnes	Besoin important
4	< 4 heures	Aucune perte d'intégrité	Donnée confidentielle restreinte aux personnes concernées	Traçabilité complète

De plus, les éléments suivants sont définis pour chaque bien :

- Durée d'Indisponibilité Maximale Autorisée (DIMA) : définit la période maximale, suite à un incident, au-delà de laquelle un service ou une donnée doit être de nouveau accessible.
- Perte de Données Maximale Autorisée (PDMA) : définit l'âge maximal des données à utiliser en remplacement de données perdues suite à un incident.
- Rétention : définit la période pendant laquelle les données doivent pouvoir être restaurées en cas de besoin.
- Propriétaire : définit la personne responsable du bien et en charge de spécifier les accès (ainsi que leurs niveaux) à celui-ci.

7 - Définition des rôles

7.1 - Incident de sécurité

Un incident de sécurité est un événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien. Il peut s'agir par exemple de l'utilisation illégale d'un mot de passe, du vol d'équipements informatiques, d'intrusion dans un fichier ou une application, …

Dans le contexte Invoke, un incident de sécurité peut porter sur des données propres à la société mais aussi sur celles d'un tiers (partenaire, client, …). Tout incident de sécurité, quelle que soit la partie impactée, est traité de manière identique par les équipes ainsi que la direction de la société.

7.2 - Rôles

Les rôles concernant la sécurité sont répartis comme suit :

- Comité de Sécurité :
  - Rédige la PSSI, la valide et la transmet à l'ensemble des Collaborateurs et personnels externes (sous-traitants, prestataires, …).
  - Gère les incidents de sécurité.
- Responsables de services :
  - Prennent connaissance de la PSSI et s'assurent de la bonne application des règles de sécurité.
  - Informent le comité de sécurité de tout incident de sécurité.

- Collaborateurs :
  - Prennent connaissance de la PSSI.
  - Informent leur responsable en cas d'incident de sécurité.

8 - Gestion de crise

Tout incident de sécurité est transmis au Comité de Sécurité qui analyse les causes et conséquences de celui-ci et prend en charge sa résolution. Afin de limiter toute compromission de l'information, cette notification d'incident est effectuée :

- Oralement auprès d'un des membres du Comité de Sécurité.
- A défaut, par téléphone auprès d'un des membres du Comité de Sécurité.

Une fois informé, et en fonction de la gravité de l'incident, le Comité de Sécurité décide de la tenue d'une réunion de gestion de crise qui donnera lieu à l'élaboration d'un plan de communication et/ou de remédiation à l'incident.

Tout incident de sécurité sur un bien, dont le facteur C (Confidentialité) est supérieur ou égal à 3, entraine obligatoirement l'information de son propriétaire sur les circonstances de l'incident ainsi que sur le plan de remédiation retenu.

9 - Principes et règles de sécurité

9.1 - Politique de sécurité

OBJECTIF :

- Doter la société d'une PSSI publiée, mise à jour régulièrement et soutenue par le Comité de Sécurité afin d'apporter à la sécurité de l'information une orientation conforme aux exigences métier et règlements en vigueur.

REGLES :

9.1.1 La PSSI, approuvée par le Comité de Sécurité, est publiée et diffusée auprès de l'ensemble des Collaborateurs et tiers concernés.

9.1.2 La PSSI s'applique à l'ensemble des utilisateurs des systèmes d'information.

9.1.3 Le document PSSI est revu et validé, a minima une fois par an, par le Comité de Sécurité.

9.1.4 La PSSI est systématiquement réexaminée à chaque changement organisationnel de l'activité ou de l'environnement technique.

9.1.5 Un plan d'action est établi après réexamen afin de combler les écarts.

9.2 - Gestion des biens

OBJECTIFS :

- Identifier et inventorier chaque bien matériel du SI.
- Identifier et inventorier chaque donnée de la société, notamment les données nécessitant une protection.

REGLES :

9.2.1 Un inventaire des biens est établi et mis à jour régulièrement (cet inventaire comprend une identification claire et documentée).

9.2.2 L'ensemble des applications installées sur les postes de travail doit être suivi et maitrisé.

9.2.3 Les responsables des biens inventoriés doivent être clairement identifiés, tout comme la personne (ou son suppléant en cas d'indisponibilité) chargée de mettre à jour les caractéristiques du bien et de maintenir des mesures de sécurité appropriées sur le bien concerné.

9.2.4 Une classification qui attribue les besoins et priorités de protection est établie pour chaque bien. Cette classification repose sur les 4 axes correspondants aux besoins en termes de Disponibilité, Intégrité, Confidentialité et Traçabilité (DICT).

9.2.5 Chaque responsable de biens doit périodiquement revoir la classification des biens dont il a la responsabilité ainsi qu'approuver les droits d'accès attribués pour ceux-ci.

9.3 - Ressources humaines

OBJECTIFS :

- Garantir que les utilisateurs connaissent les responsabilités en termes de sécurité.

- Réduire les risques d'accident, d'erreur et/ou de malveillance en intégrant les principes de sécurité dans la gestion des ressources humaines, du recrutement à la fin de la collaboration.
- Veiller à ce que les Collaborateurs quittent la société ou changent de poste selon une procédure définie et diffusée.

REGLES :

9.3.1 Une clause de confidentialité rappelant les obligations en matière de secret professionnel concernant les données de la société et de sa clientèle est intégrée au contrat de travail de chaque collaborateur.

9.3.2 En cas de non-respect de la PSSI, des mesures disciplinaires seront, le cas échéant, prises conformément aux règles contenues dans le règlement intérieur de la société.

9.3.3 Les utilisateurs sont régulièrement sensibilisés à la sécurité par le biais de communications dont ils doivent avoir pris connaissance.

9.3.4 Une procédure de départ ou de changement de poste est formalisée et comprend :

- La suppression des droits d'accès.
- La reprise des matériels.
- La suppression ou l'archivage des données de l'utilisateur en cas de non reprise par un remplaçant.

9.3.5 Une procédure d'accès aux données personnelles d'un collaborateur (fichiers, emails, …) en cas de défaillance de ce dernier (indisponibilité, maladie, …) est formalisée.

9.3.6 Les informations concernant les utilisateurs accédant à des données sensibles sont vérifiées ou attestées avant toute autorisation d'accès.

9.4 - Sécurité physique et environnementale

OBJECTIF :

- Veiller que seules les personnes habilitées ont accès aux bâtiments, locaux techniques.

REGLES :

9.4.1 Seules les personnes habilitées peuvent accéder aux différents sites de la société. Les Collaborateurs se voient attribuer un badge ou clé

personnels leur permettant d'accéder uniquement aux salles et bureaux pour lesquels ils sont autorisés d'accès.

9.4.2 Les visiteurs sont escortés par une personne habilitée qui assume la responsabilité de leurs actions.

9.4.3 L'accès aux locaux techniques n'est autorisé qu'aux personnes habilitées par la Direction des Systèmes d'Information.

9.5 - Protection des matériels et supports papier

OBJECTIFS :

- Assurer la protection et la disponibilité des équipements sensibles.
- Assurer une sécurité homogène (incendie, climatisation, inondation) des salles serveurs.

REGLES :

9.5.1 Les éléments non dématérialisés, comme les dossiers papier ou archives, doivent être stockés dans des locaux adéquats, afin de les protéger contre le vol, les incendies, l'humidité et les inondations.

9.5.2 Les règles relatives au cycle de vie des supports papiers (création, copie, stockage, transmission, exploitation et destruction) selon leur niveau de confidentialité sont à appliquer selon les exigences de classification.

9.5.3 Tous les équipements informatiques qui sont répertoriés comme importants ou vitaux pour la société sont installés dans des locaux sûrs.

9.5.4 La protection des équipements sensibles est réalisée par des mesures de prévention et/ou de protection en fonction de leur sensibilité (protection incendie, climatisation, secours électrique par onduleur).

9.5.5 Des entretiens réguliers des solutions de protection physique des salles serveurs sont réalisés périodiquement par les équipes internes ou par des sociétés de maintenance tierces qualifiées et habilitées pour ces opérations.

9.5.6 Pour les biens classifiés sensibles, un contrat de maintenance est conclu avec un délai d'intervention ou de remplacement garanti, compatible avec les exigences de disponibilité et d'intégrité.

9.6 - Procédures et responsabilités liées à l'exploitation

OBJECTIF :

- Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.

REGLES :

9.6.1 Les procédures d'exploitation (système, réseau, poste de travail, application) sont formalisées, partagées et les responsabilités associées (suivi, approbation, mise à jour) sont définies.

9.6.2 La documentation des Systèmes d'Information (architecture, fonctionnement, procédures) est sauvegardée et son accès est réservé au personnel habilité.

9.6.3 Chaque action menée sur les biens (mises à jour, modification de paramètres, erreurs rencontrées et corrections menées) est inscrite et tracée dans un outil de suivi.

9.6.4 L'administration des infrastructures critiques directement depuis les postes de travail est interdite. Ces actions sensibles s'effectuent depuis un composant déterminé.

9.6.5 Le processus de modifications majeures des Systèmes d'Information (ouverture vers l'extérieur, modification de l'architecture, ajout d'une application critique) doit faire l'objet d'une analyse des risques et d'une validation du responsable DSI.

9.6.6 Aucun accès à des tiers n'est autorisé sur les interfaces d'administration des infrastructures critiques.

9.7 - Sécurité liée à l'exploitation

OBJECTIFS :

- Suivre les événements systèmes
- Assurer le bon fonctionnement des SI
- Détecter et analyser un dysfonctionnement
- Détecter, analyser et remédier les vulnérabilités

REGLES :

9.7.1 Les équipements des Systèmes d'Information sont surveillés en temps réel. Les principales informations concernant l'état du matériel, la disponibilité des services et les ressources utilisées sont consolidées. En

cas de dysfonctionnement, une alerte est automatiquement remontée aux équipes techniques pour traitement.

9.7.2 Le traçage des événements (ou logs) sur les systèmes doit être activé partout où il est disponible et pertinent.

9.7.3 La collecte et la conservation des traces doivent être faites de manière à permettre leur utilisation comme élément de preuve aussi probant que possible. La conservation des traces doit comporter au minimum les 180 derniers jours pour les biens sensibles.

9.7.4 Le processus de gestion des changements (mise à jour des correctifs et mise à jour de sécurité) est formalisé et mis en production sur l'ensemble des équipements systèmes, réseaux, des postes de travail et des logiciels.

9.7.5 Les matériels et systèmes obsolètes doivent être clairement identifiés et doivent faire l'objet d'une analyse des risques par l'équipe en charge.

9.7.6 Des scans sont réalisés périodiquement sur l'ensemble des équipements afin de détecter les vulnérabilités exploitables sur ces derniers.

9.7.7 Une veille est réalisée, auprès des éditeurs des solutions tierces utilisées, concernant les vulnérabilités et correctifs de sécurité publiés par ceux-ci.

9.7.8 Les vulnérabilités exploitables doivent être traitées de manière proportionnée au risque.

9.7.9 Toute vulnérabilité exploitable et présentant un risque avéré pour le bon fonctionnement, la disponibilité ou confidentialité des SI ou des biens est traitée, au plus tard, dans les 24 heures suivant sa découverte.

9.8 - Protection contre les malveillances

OBJECTIFS :

- Protéger l'intégrité des logiciels et de l'information.
- Contrôler et filtrer l'accès Internet.

REGLES :

9.8.1 Tous les serveurs et postes de travail doivent être protégés et supervisés afin de garantir l'intégrité des informations (données, configuration, etc.).

9.8.2 Les protocoles réseaux autorisés et non autorisés doivent être identifiés et mis en production sur les équipements de sécurité périmétrique et de réseaux internes permettant leur cloisonnement.

9.8.3 Toute connexion distante aux outils de la société doit être réalisée en utilisant une solution permettant le chiffrement des flux.

9.8.4 Toute authentification (couple login/mot de passe) doit être chiffrée afin de rendre impossible l'interception des informations d'authentification d'un utilisateur.

9.8.5 La liste des flux réseaux entrants et sortants autorisés est formalisée. Tous les flux n'étant pas décrits dans ce référentiel sont interdits.

9.8.6 Les éléments de maintenance comme des patchs ou mises à jour doivent être émis par une source fiable et l'intégrité des éléments contrôlés. Autant que possible, ces éléments seront recueillis au travers d'une zone réseau dédiée à cet effet.

9.8.7 Les connexions Internet des utilisateurs sont filtrées et journalisées. Une liste des sites non autorisés est établie et remise à jour régulièrement.

9.9 - Sauvegarde

OBJECTIF :

- Maintenir l'intégrité et la disponibilité des informations et garantir leur restauration.

REGLES :

9.9.1 Pour chaque bien, une politique de sauvegarde est formalisée et validée, prenant en compte :

- le responsable de la sauvegarde,
- la fréquence et le type (complète, incrémentale, différentielle),
- le support (bande, disque),
- la durée de rétention,
- la périodicité des tests de restauration.

9.9.2 Les données sauvegardées doivent être délocalisées dans un local sécurisé distant de l'environnement de production.

9.9.3 La politique de sauvegarde est régulièrement revue et mise à jour par les responsables et/ou équipes techniques.

9.9.4 Les Collaborateurs doivent réaliser des sauvegardes régulières en utilisant les espaces de stockage sécurisés mis à leur disposition et en excluant tout recours à des périphériques de stockage externe (cloud public, clé USB, …).

9.10 - Sécurité de l'information et des supports

OBJECTIFS :

- Garantir la confidentialité des données stockées et échangées en interne ou avec des tiers.
- Empêcher la divulgation, la modification, le retrait ou la destruction non autorisée de biens.

REGLES :

9.10.1 Les propriétaires d'information doivent définir les autorisations d'accès aux informations et distinguer les droits en lecture seule ou en lecture/écriture.

9.10.2 Les utilisateurs doivent être sensibilisés à la mise en œuvre d'un ensemble de bonnes pratiques concernant les protections des biens sensibles, comme par exemple :

- Le stockage de leurs données sensibles sur des supports adaptés en termes de sécurité.
- La destruction systématique des documents sensibles est réalisée à l'aide de broyeurs.
- Les documents ne sont pas laissés sur les imprimantes, copieurs ou fax.
- Les documents, s'ils doivent être conservés, sont stockés en armoire ou coffre-fort.

La politique de classification précise l'ensemble des règles applicables aux informations selon leur cycle de vie et niveau de confidentialité.

9.10.3 Les utilisateurs ne doivent pas stocker sur un support nomade (PC portable, clé USB, …) des données sensibles (internes ou externes), sauf à obtenir l'autorisation explicite du propriétaire. Il en va de même pour les espaces de stockage en ligne, externes à la société (notamment les clouds publics).

9.10.4 Le processus de restitution des biens est formalisé et prévoit la remise de l'ensemble des biens appartenant à la société ainsi que la suppression sécurisée des données présentes sur l'ensemble des supports avant réattribution.

9.10.5 Lors du remplacement ou de la mise au rebut d'un bien équipé d'un support de stockage, ce dernier doit faire l'objet d'une gestion particulière incluant la destruction définitive et sécurisée des données qu'il contient.

9.10.6 Les équipements nomades (PC, tablettes, …) doivent disposer d'un système de chiffrement du stockage interne activé et contrôlé.

9.11 - Contrôle d'accès

OBJECTIFS :

- Garantir un contrôle efficace d'accès aux informations.
- Suivre et maîtriser les accès au SI.

REGLES :

9.11.1 L'identification de la personne se connectant au réseau est effectuée de façon formelle et non ambiguë. L'ensemble des utilisateurs des SI (interne, tiers, ...) possède un compte nominatif.

9.11.2 Les personnes habilitées ayant des pouvoirs étendus disposent chacun d'un compte différent de leur compte utilisateur standard. Les comptes à privilèges respectent la règle précédente.

9.11.3 Toute création, modification et clôture de compte doit pouvoir être suivie et tracée.

9.11.4 L'ensemble des accès au SI est tracé.

9.11.5 La collecte et la conservation des accès doivent être faites de manière à permettre leur utilisation comme élément de preuve.

9.11.6 La procédure des mouvements (arrivée, départ ou mutation interne) est formalisée et inclut la mise à jour du référentiel et des droits d'accès associés.

9.11.7 Une politique de mots de passe complexes ciblant l'ensemble des utilisateurs des SI est mise en place et respecte les préconisations relatives à la sécurité :

- Processus de remise du mot de passe.

- Complexité (longueur minimale, utilisation de types de caractères différents).
- Interdiction de réutilisation d'anciens mots de passe.
- Limite de tentatives d'accès.
- Verrouillage automatique.
- Renouvellement obligatoire après une période d'expiration prédéfinie.

9.11.8 Des dispositifs limitant les autorisations d'accès sont mis en œuvre pour assurer la protection de l'accès aux Systèmes d'Information :

- Verrouillage automatisé des sessions après une période d'inactivité.
- Le verrouillage manuel des sessions est encouragé lorsque l'utilisateur quitte son poste de travail.

9.12 - Acquisition, développement et maintenance des Systèmes d'Information

OBJECTIFS :

- Garantir la gestion de la sécurité tout au long du cycle de vie des Systèmes d'Information.
- Réduire les risques liés à l'exploitation des vulnérabilités techniques et applicatives.

REGLES :

- Les développements et les acquisitions doivent prendre en compte les besoins des métiers en matière de sécurité. Une analyse des besoins de sécurité doit être effectuée suivant l'échelle des besoins de sécurité (cf. 6 - Les besoins de sécurité).

9.12.1 Des audits de vulnérabilités sont effectués sur les applications, bases de données et systèmes sensibles :

- Dans le cadre de leur mise en place.
- A intervalle régulier.
- En cas d'évolution majeure du système d'exploitation, de l'application ou de la configuration matérielle.
- En cas d'apparition d'une nouvelle vulnérabilité majeure, dans le but de confirmer ou rejeter son exploitabilité.

9.12.2 Le processus de mise en production d'une application ou d'un système prévoit la mise en place de plusieurs environnements et impose la séparation de ceux-ci (développement, recette, production).

9.13 - Gestion des incidents

OBJECTIFS :

- Garantir la mise en place d'une politique cohérente et efficace pour la gestion des incidents liés à la sécurité de l'information.
- Garantir la remontée des événements et failles de sécurité.
- Permettre la mise en œuvre d'actions correctives ou préventives dans les meilleurs délais.

REGLES :

9.13.1 En cas d'infection (vers, virus, cheval de Troyes), faille de sécurité ou incident de sécurité constaté ou soupçonné sur un poste de travail, une procédure de réaction connue de tous les utilisateurs est mise en œuvre.

9.13.2 Une surveillance permanente des systèmes, des alertes et des vulnérabilités est mise en œuvre afin de détecter les dysfonctionnements liés à la sécurité de l'information.

9.13.3 Des indicateurs sont mis en place et permettent de recenser les incidents, l'origine, la cause, l'impact sur la disponibilité, l'intégrité, la preuve ou la confidentialité.

9.13.4 L'analyse des incidents de sécurité donne lieu à un plan d'actions (préventives ou curatives) permettant d'améliorer les mesures existantes, et, selon le besoin, d'en créer de nouvelles.

9.14 - Gestion de la continuité d'activité informatique

OBJECTIFS :

- Suite à un incident mineur (panne d'équipement), assurer le secours informatique en fonction des besoins des métiers.
- Suite à un incident majeur impactant l'ensemble d'une salle serveurs, assurer une continuité d'activité informatique des biens sensibles dans les meilleurs délais en fonction des besoins des métiers.

REGLES :

9.14.1 Les besoins en termes de secours informatique et de Continuité d'Activité, à savoir la Durée Maximale d'Interruption Autorisée (DIMA) et la Perte de Données Maximale Autorisée (PDMA) doivent être intégrés dans les nouveaux projets.

9.14.2 S'agissant des biens sensibles, les plans de secours informatique après incidents sont définis par les différentes équipes informatiques.

9.14.3 Les procédures et solutions de secours informatique sont régulièrement testées par les équipes informatiques.

9.14.4 Un Plan de Continuité d'Activité (PCA), en cas de problème majeur impactant l'ensemble d'une salle machines (coupure électrique, incendie, …), est défini et disponible dans le cadre de la documentation sécurité.

9.14.5 Un exercice annuel du PCA doit être planifié et réalisé.

9.15 - Conformité

OBJECTIF :

- Eviter toute violation de la propriété intellectuelle, des obligations contractuelles et des exigences de sécurité.

REGLES :

9.15.1 L'application de la PSSI fait l'objet d'un suivi et d'un contrôle régulier. Le Comité de Sécurité a la capacité d'effectuer des contrôles inopinés sur tout élément des SI de la société pour en vérifier la conformité.

9.15.2 Des logiciels de contrôle non intrusifs peuvent être activés sur les postes et serveurs afin de vérifier la conformité de ceux-ci.

9.15.3 Un inventaire et un suivi de l'installation des logiciels demandant l'achat d'un droit d'usage est réalisé.

9.15.4 Des contrôles permettant de s'assurer que le nombre maximal d'utilisateurs habilités n'est pas supérieur au nombre de licences acquises sont effectués.

9.15.5 Les logiciels créés par un employé (à durée indéterminée ou temporaire) dans le cadre de son contrat de travail ou d'un stagiaire dans le cadre de son stage, sont la propriété d'Invoke. Ces éléments sont intégrés dans les contrats et les conventions de stage.

9.16 - Données personnelles

OBJECTIF :

- Adopter une politique cohérente pour le stockage et le traitement des données personnelles en prenant en compte la règlementation européenne sur la protection des données personnelles (RGPD) afin de répondre à l'ensemble de ses nouvelles obligations en tant que :
  - Responsable de traitement concernant les traitements relatifs au fonctionnement de l'entreprise ;
  - Sous-traitant pour les traitements relevant de son activité auprès de sa clientèle.

REGLES :

9.16.1 Les traitements impliquant des données personnelles doivent être identifiés.

9.16.2 La collecte de données personnelles ne comprend pas d'éléments non nécessaires au traitement réalisé.

9.16.3 Les données personnelles ne sont pas conservées lorsqu'elles ne sont plus utiles au traitement réalisé.

9.16.4 Toute demande de consultation, modification ou suppression des données personnelles, dont Invoke est responsable du traitement, par un utilisateur est traitée dans un délai ne pouvant excéder un mois.

9.16.5 Les données personnelles ne sont ni stockées ni transmises hors de l'Union Européenne.

9.16.6 La protection des données personnelles donne lieu à plusieurs documents dédiés :

- Protection des données personnelles applicable au Service SaaS, à la réalisation de Services Professionnels et au Support ;
- Information auprès des Collaborateurs ;
- Protection des données personnelles demandée aux sous-traitants lorsque Invoke est Responsable de traitement.

9.17 - Cryptographie

OBJECTIFS :

- Assurer une sécurisation des flux cohérente avec les objectifs métiers et de confidentialité
- Définir une politique de gestion des clés de chiffrement

REGLES :

9.17.1 Les supports de stockage des PC utilisateurs doivent utiliser un système de chiffrement fiable, géré et contrôlé de manière centralisée.

9.17.2 Le chiffrement symétrique doit être assuré par une taille de clé de 128 bits ou supérieur. Autant que possible, une méthode de chiffrement par bloc avec vérification d'intégrité sera préférée comme AES CBC-MAC.

9.17.3 La taille des empreintes sera au minimum de 256 bits. A minima, le mécanisme de hachage SHA-256 conforme au référentiel FIPS 180-2 est à utiliser.

9.17.4 La taille minimale du module sera de 2048 bits pour les algorithmes par factorisation comme RSA 2048, ou Diffie-Hellman groupe 14. Pour les algorithmes à courbes elliptiques l'ordre du sous-groupe doit être multiple d'un nombre premier d'au moins 250 bits comme Diffie-Hellman groupe 19.

9.17.5 Toute non-conformité ou défaillance du chiffrement doit faire l'objet d'une alerte remontée aux services techniques et être gérée comme un incident de sécurité.

9.17.6 L'accès aux clés de chiffrement doit être limité aux seules personnes habilitées et pour lesquelles cet accès est nécessaire dans le cadre de leur mission.

9.17.7 Toute divulgation d'une clé de déchiffrement doit entrainer la révocation de cette clé et son remplacement immédiat.

9.17.8 Les données sensibles qui transitent sur les réseaux (publics ou internes) doivent obligatoirement être chiffrées.

9.17.9 Seuls les protocoles, algorithmes et suites de chiffrement non obsolètes et garantissant une sécurisation forte des échanges doivent être utilisés. Ceux ne respectant pas l'état de l'art doivent être désactivés ou faire l'objet d'une analyse de risque en conséquence.

9.17.10 Les emails entrants ou sortants doivent être chiffrés dès lors que les serveurs partenaires le permettent. Il doit être possible de rendre obligatoire ce chiffrement pour certains partenaires lorsque la sensibilité des données échangées le nécessite.

9.17.11 L'accès par un tiers (client, partenaire, …) à une ressource hébergée par Invoke au travers des réseaux publics doit être sécurisé par l'utilisation de certificats émis par une autorité de confiance tierce reconnue.