Politique de sécurité des systèmes d'informations

Historique des modifications

Version	Objet de la modification	Statut
19/04/2021 (1.0)	Rédaction de la politique de sécurité des systèmes d'information (PSSI)	Draft

Table des matières

Eléments stratégiques

Périmètre de la PSSI

La sécurité des systèmes d'information (SSI) de Soft Concept couvre l'ensemble des systèmes d'information de l'entreprise avec toute la diversité que cela implique dans les usages, les lieux d'utilisation, les méthodes d'accès, les personnes concernées...

Il a pour but de protéger :

- Le système informatique interne de l'entreprise
- Les données interne de l'entreprise (mail, code source, sauvegarde…)
- Les serveurs d'hébergements
- Les librairies scientifiques et techniques développés par l'entreprise
- Les informations relatives aux personnes physiques et morales avec qui l'entreprise est en relation.

Enjeux et orientations stratégiques

La sécurité du Système d'information repose sur les critères suivants :

Critères de sécurité	**Définitions**
Confidentialité	Propriété accessible qu'aux utilisateurs autorisées.
Disponibilité	Propriété accessible au moment voulu.
Fiabilité	Propriété exacte par rapport à son utilisation.

Les besoins de sécurité s'appliquent aussi bien aux ressources du système d'information (postes informatiques, réseaux, applications…) qu'aux données traitées par ces ressources.

Aspects légaux et règlementaire

Le système d'information et les applications proposées par Soft Concept respectent les lois sur la protection de la vie privée :

- Articles 226-1 à 226-8 du Code pénal
- Articles R 226-1 à R 226-12 du Code pénal
- Article 9 du Code civil
- Règlement (UE) 2016/679 (RGPD)

Référentiel légal et réglementaire pour la protection du secret professionnel :

- Articles 226-13, 226-14 du Code pénal

Référentiel légal et réglementaire concernant la protection du secret de la correspondance :

- Articles 226-15, 432-9 du Code pénal
- Loi n°91-646 du 10 juillet 1991

Echelle de besoins

L'échelle des besoins présenté ici permet d'apporter une pondération et des valeurs de références par rapport aux critères de sécurité choisis, ainsi qu'une liste d'impact enrichis d'exemples.

Echelle de confidentialité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveaux de l'échelle	Description détaillée de l'échelle
1 : Public	Le domaine est public.
2 : Limité	Le domaine n'est accessible qu'au personnel et aux partenaires.
3 : Réservé	Le domaine n'est accessible qu'au personnel (interne) impliquées.
4 : Privé	Le domaine n'est accessible qu'à des personnes identifiées et en ayant le besoin.

Echelle de disponibilité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveaux de l'échelle	Description détaillée de l'échelle
1 : Plus de 72h	Le domaine peut être indisponible plus de 72 heures.
2 : Entre 24 et 72h	Le domaine doit être disponible dans les 72 heures.
3 : Entre 4 et 24h	Le domaine doit être disponible dans les 24 heures.
4 : Moins de 4h	Le domaine doit être disponible dans les 4 heures.

Echelle de fiabilité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de fiabilité :

Niveaux de l'échelle	Description détaillée de l'échelle
1 : Développement	La fiabilité du domaine n'est pas assurée.
2 : Détectable	Les sources de non-fiabilités du domaine sont identifiées.
3 : Maitrisé	Les sources de non-fiabilités sont identifiées et la fiabilité essentielle du domaine est présent.
4 : Fiable	Le domaine est rigoureusement fiable.

Impact :

Les impacts pour l'entreprise sont de multiples natures. Ces impacts reflètent les axes importants et justifient les besoins de sécurités énoncés.

Il s'agit de :

- La perte d'image de marque. Une trop faible importance des besoins de fiabilités peut entrainer un manque de confiance de la part des clients et avec le départ de ceux-ci.
- Pertes financières. Le manque de fiabilité ou de disponibilité des produits peut impacter les ventes de ces produits.

Besoins de sécurité

Pour chacun des domaines d'activités et chaque critère de sécurité précédemment énoncé, une valeur correspondant à l'échelle des besoins pour les impacts retenus est déterminée. Ces valeurs sont renseignées dans le tableau ci-dessous.

Domaine	Confidentialité	Disponibilité	Fiabilité
Serveurs	4	4	4
Réseau interne	4	4	4
Poste de travails	2	3	2
Librairies développées	4	1	3
Sources applications	4	1	3
Documentation	3	3	2
Formations	3	2	3

Origine des menaces

Les menaces pesant sur la PSSI sont regroupées dans le tableau suivant :

Menace	Cause	Impacts
Gestion des serveurs		
Indisponibilité des serveurs	• Employé peu sérieux • Incendie des locaux • Panne de courant • Usure du matériel • Virus non ciblé	• Perte de crédibilité
Altération des serveurs	• Employé peu sérieux • Matériel dégradé • Virus non ciblé	• Perte de crédibilité
Destruction des serveurs	• Incendie des locaux • Virus non ciblé	• Perte de crédibilité
Réseau		
Indisponibilité du réseau interne	• Panne de courant • Usure du matériel	• Pas d'accès aux données de l'entreprise
Indisponibilité du réseau internet	• Panne de courant • Problème fournisseur d'accès	• Pas de d'accès à internet • Serveurs indisponibles
Perte d'information/document	• Employé peu sérieux • Virus non ciblé	• Perte de données entreprise

Pour chaque menace, il est nécessaire d'en évaluer le risque, de considérer la probabilité que celle-ci devienne réalité et détecter les éventuels facteurs aggravants (négligence constatée, insuffisance d'information, de consignes…).

Règles de sécurité

Organisation

Le système d'information de l'entreprise étant sujet à modification, il est prévu de réexaminer la PSSI :

- Lors de toute évolution majeure du contexte ou du SI,

- Dans le cas d'une évolution de la menace,
- Dans le cas d'une évolution des besoins de sécurité,
- A la suite d'un audit,
- A la suite d'un incident de sécurité.

La PSSI ainsi que toutes ses déclinaisons opérationnelles doivent être parfaitement documentées et les versions de références à jour doivent être facilement accessibles à tous les personnels de l'entreprise.

Afin d'éviter les indiscrétions et les fuites, les informations ne doivent pouvoir être utilisés que dans un environnement répondant aux exigences de sécurité définies par l'entreprise.

Au sein de l'entreprise, la responsabilité générale de la sécurité des systèmes d'information relève du PDG en tant qu'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI). Il est assisté dans cette fonction par le Responsable de la Sécurité des Systèmes d'Information (RSSI).

Mise en œuvre

La PSSI de l'entreprise affiche un ensemble de principes d'ordre organisationnel et technique à caractère prioritaire. Ces principes sont explicités, voire complétés, dans le cadre d'instructions ou dispositions techniques dont la responsabilité d'élaboration, de diffusion et d'information relève de la chaîne fonctionnelle SSI.

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) exerce sous l'autorité directe du PDG de l'entreprise, les activités suivantes :

- Contribuer activement à l'élaboration d'une politique de sécurité cohérente admise par tous et la mettre en œuvre.
- Viser tous les projets de l'établissement afin de veiller à la mise en œuvre au sein de ces derniers des éléments technologiques nécessaires à l'application de la PSSI.
- Coordonner, animer le réseau des correspondants sécurité de l'établissement.
- Proposer et mettre en œuvre des actions de sensibilisation et d'information de tous les utilisateurs aux aspects sécurité des systèmes d'information.

L'accès extérieur aux postes de travail doit demeurer l'exception et être justifiée en termes de besoins et de compétences.

Technique

Le traitement et le stockage des données numériques, l'accès aux applications et services et les échanges de données entre systèmes d'information doivent être réalisés selon des méthodes visant à prévenir la perte, la modification et la mauvaise utilisation des données ou la divulgation des données ayant un caractère sensible.

Plan d'action

Sauvegardes et Environnement

Une sauvegarde régulière des données avec des processus de restauration régulièrement validés doit être mise en place. On distinguera les sauvegardes de production (par exemple, restauration d'une donnée) des sauvegardes de recours (par exemple, reprise des services sur des moyens externes à la suite d'incident majeur). Une étude des données (criticité, volatilité, fluctuation…) permettra de définir la périodicité et le type de sauvegarde ainsi que la durée de rétention dans le respect des législations en vigueur.

Gestion des Equipements

L'administration des serveurs de l'entreprise est placée sous la responsabilité d'un administrateur systèmes et réseaux.

L'administration des postes de travail individuels est placée sous la responsabilité des utilisateurs.

L'administrateur systèmes et réseaux peut intervenir à distance pour des opérations de maintenance sur le poste de travail d'un utilisateur après l'en avoir averti et en respectant les principes de la loi Informatique et Libertés.

L'utilisation des moyens informatiques est limitée aux seules missions de Soft Concept et aux besoins de l'activité qui en découle. L'utilisateur doit se conformer aux dispositions des responsables informatiques.

Isolement des Flux

Les serveurs doivent être protégés spécifiquement vis-à-vis des postes de travail et des autres serveurs. On distinguera les serveurs accessibles uniquement à partir du réseau de l'entreprise et ceux accessibles aussi de l'extérieur.

Par principe, les flux de réseau doivent être limités au strict nécessaire.

Les accès à distance des collaborateurs au réseau de l'entreprise ne sont pas autorisés.

Toute connexion de tiers (clients, partenaires) au réseau de l'entreprise est interdite.

Gestion des Accès

Toute utilisation d'accès au SI est soumise à une autorisation personnelle et incessible accordée par le DG de Soft Concept. Chaque utilisateur dispose d'un identifiant et mot de passe. Le collaborateur est responsable de toute utilisation faite à partir de ses identifiants.

Soft Concept autorise l'accès au SI et aux données exclusivement aux collaborateurs concernés dans le cadre de leurs fonctions.

Le DPO est chargé de gérer les habilitations. Il s'engage notamment à définir les profils d'habilitation, supprimer les permissions d'accès obsolètes (par exemple lors du départ d'un salarié, ou un changement de poste).

Protection du matériel informatique

Chaque utilisateur est responsable de la mise à jour des logiciels antivirus présent sur son poste de travail ainsi que des mises à jour de sécurité de son système d'exploitation.

L'utilisateur doit veiller à verrouiller sa session dès lors qu'il quitte son poste de travail. Les postes individuels sont toutefois protégés par un verrouillage automatique de session.

Une mise à jour automatique du système d'exploitation des serveurs est prévue tous les mois.

Sécurité physique du système d'information

Soft Concept restreint l'accès à l'ensemble des locaux au moyen de portes verrouillées. Les collaborateurs habilités ont accès aux locaux au moyen d'un badge magnétique.

Si un collaborateur identifie un inconnu non accompagné ou non autorisé dans les locaux de Soft Concept, il doit immédiatement prévenir le DPO.

Les postes de travail sont les points d'entrée principaux du système d'information. Les utilisateurs sont sensibilisés à rendre leur environnement de travail inaccessible en leur absence (verrouillage de la session, arrêt du poste de travail, utilisateur temporaire). Pour renforcer cette mesure et éviter des négligences, des

mesures de protection automatique d'une session de travail après un délai d'inactivité ont été mis en place (déconnexion automatique).