Politique de sécurité des systèmes d'information (PSSI)

La PSSI est un texte de référence qui définit les règles, principes et objectifs de sécurité informatique dans une organisation.

1. Contexte

noesya est une très petite entreprise (TPE, moins de 10 personnes salariées) coopérative. L'équipe est répartie entre deux lieux physiques, à Bordeaux et à Paris. Les personnes pratiquent le télétravail partiel.

2. Périmètre de la SSI

La sécurité des systèmes d'information (SSI) de noesya 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, ainsi que les applications institutionnelles (messagerie, applications, stockage, sauvegarde…).

3. Besoins de sécurité

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

- Confidentialité : « La confidentialité est la propriété qu'une information n'est ni disponible ni divulguée aux personnes, composantes ou processus non autorisés » norme ISO 7498-2 (ISO90).

- Disponibilité : Propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs autorisés.

- Intégrité : « L'intégrité est la prévention d'une modification non autorisée de l'information » norme ISO 7498-2 (ISO90).

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. Il est nécessaire d'inventorier et de classifier ces données afin d'en identifier le degré de sensibilité et donc le besoin de protection nécessaire.

4. Menaces

Afin de mettre en place les moyens de sécurité adéquates, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité – DCSSI) préconise de connaître les typologies de menaces et leurs impacts.

On distingue ainsi :

- les attaques visant directement le système d'information : vol de données (et éventuellement les ressources supportant ces données), modification des données, déni de service…

- les attaques visant les ressources informatiques : vol de ressources, détournement des ressources, altération des données, émission de malware…

- les accidents : sinistres naturels, altération accidentelle des données ou ressources…

Pour chaque menace, il est alors nécessaire d'en évaluer le risque, donc de considérer la probabilité que celle-ci devienne réalité et détecter les éventuels facteurs aggravants.

5. Pilotage

noesya ne dispose pas de Responsable de la Sécurité des Systèmes d'Information (RSSI) dédié.

Au sein de noesya, la responsabilité générale de la sécurité des systèmes d'information relève conjointement de tous les salarié·e·s développeur·es.

6. Mise en œuvre de la PSSI

La PSSI de noesya affiche un ensemble de principes d'ordre organisationnel et technique à caractère prioritaire.

7. Organisation et responsabilités

7.1. Responsabilité des différents acteurs

Les acteurs intervenant en matière de sécurité des systèmes d'information doivent être informés de leurs responsabilités en matière de SSI. Dans l'exercice de leur activité, ils sont liés à leur devoir de réserve voire à des obligations de secret professionnel.

7.2. Accès aux ressources informatiques

La mise à disposition d'un utilisateur de moyens informatiques doit être formalisée à l'arrivée, au changement de fonction et au départ de l'intéressé. L'accès aux ressources doit être contrôlé (identification, authentification) et adapté au droit à en connaître de l'utilisateur (droits et privilèges, profil utilisateur).

7.3. Charte informatique

Préalablement à son accès aux outils informatiques, l'utilisateur doit prendre connaissance des droits et devoirs que lui confère la mise à disposition par sa composante de ces outils. Cette information se fait par le biais d'une formation spécifique effectuée lors de l'onboarding de l'utilisateur.

7.4. Cyber surveillance

La sécurité des systèmes d'information exige de pouvoir surveiller le trafic sur le réseau et tracer les actions effectuées. Les dispositifs mis en œuvre doivent être conformes à la réglementation en vigueur et respecter les principes de proportionnalité (adaptation du niveau des moyens à l'enjeu effectif de la sécurité) et de transparence (information des utilisateurs).

8. Protection des données

8.1. Disponibilité, confidentialité et intégrité des données

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.

Une sauvegarde régulière des données avec des processus de restauration régulièrement validés doit être mise en place. Une étude fine 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.

8.2. Protection des données sensibles

noesya n'a jamais accès à des données « classifiées de défense ».

Les données non classifiées mais présentant un caractère sensible doivent être identifiées et le cas échéant repérées selon un niveau de sensibilité ; il sera procédé régulièrement à un réexamen de la sensibilité des données. Ces données devront faire l'objet d'une protection au niveau du contrôle d'accès (authentification et contrôle d'autorisation), du traitement, du stockage ou de l'échange (chiffrement) pour en assurer la confidentialité.

Avant toute cession ou mise au rebut d'un matériel ayant contenu des données sensibles, il est nécessaire de s'assurer que toutes les données ont bien été effacées par un procédé efficace et selon les recommandations techniques nationales. Si cela s'avère impossible les supports concernés devront être détruits.

8.3. Données à caractère personnel

Les traitements de données susceptibles de contenir des informations à caractère personnel (au sens de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) doivent faire l'objet des formalités requises de déclaration ou de demande d'autorisation auprès de la CNIL, via la correspondant CIL de l'établissement.

Les données à caractère personnel constituent des données sensibles et comme telles doivent faire l'objet de protection.

8.4. Chiffrement

Le chiffrement, en tant que moyen de protection, est obligatoire pour le stockage et l'échange de données sensibles.

9. Sécurisation du Système d'information

9.1. Administration des serveurs

noesya ne dispose d'aucun serveur propre.

9.2. Administration des postes de travail

L'administration des postes de travail individuels est placée sous la responsabilité des utilisateurs eux-mêmes, après mise en pratique de la formation reçue lors de l'onboarding.

9.3. Sécurisation des postes de travail et des moyens nomades

La sécurisation des postes de travail et des moyens nomades est placée sous la responsabilité des utilisateurs.

L'accès aux postes de travail et moyens nomades doit être protégé par mots de passe suffisamment robustes ; chaque mot de passe est personnel et confidentiel et, à ce titre, il ne doit pas être divulgué à un tiers, quel qu'il soit, ni laissé sans protection.

Les utilisateurs veillent au bon déroulement des applicatifs de sécurisation installés sur les moyens informatiques mis à leur disposition : mises à jour effectives de l'anti-virus, du système d'exploitation et des applications présentes.

En particulier, les utilisateurs prendront des mesures spécifiques adaptées en cas d'utilisation des moyens nomades en dehors de leur zone de sécurité (protection contre le vol, chiffrement…).

9.4. Contrôle d'accès

Tout accès au système d'information est soumis à l'identification/authentification du demandeur et au contrôle de ses autorisations/habilitations. Il importe de bien définir les autorisations et de n'attribuer que les privilèges nécessaires. Les accès doivent être journalisés. L'utilisation de comptes partagés ou anonymes doit demeurer l'exception et être justifiée en termes de besoins.

L'attribution et la modification des accès et privilèges d'un applicatif doivent être validées par le responsable de l'applicatif.

9.5. Sécurité des applications

Les applications internet utilisées dans l'entreprise, doivent être sécurisées, en cohérence avec la sensibilité des informations traitées et échangées.

Applications dans le cloud

noesya a recourt à de nombreuses applications dans le cloud, notamment pour la gestion de ses emails et le stockage de ses données. noesya s'assure que le prestataire choisi pour ces applications est compatible avec la présente PSSI.

10. Mesure du niveau effectif de sécurité

10.1. Audits

Le niveau de sécurité des systèmes d'information et la conformité de mise en œuvre des recommandations sur le terrain peuvent donner lieu à des audits internes.

10.2. Journalisation, tableaux de bord

Le système d'information doit comprendre des dispositifs de journalisation centralisée et protégée. L'objectif est de permettre de détecter des intrusions ou des utilisations frauduleuses, de tenter d'identifier les causes et les origines, d'éviter des contaminations d'autres sites par rebond et de remettre en place le système. Conformément à la législation française, ces informations peuvent faire l'objet d'une transmission aux autorités compétentes.

La durée de conservation des fichiers de traces à des fins de preuve doit être conforme aux lois et règlements en vigueur.

Il importe de définir, et de faire connaître aux utilisateurs, les règles d'exploitation des fichiers de traces (contenu, durée de conservation, utilisation) dans le respect du « principe de proportionnalité » et des contraintes législatives et réglementaires concernant notamment le traitement des informations à caractère personnel.

10.3. Gestion d'incidents

Chaque acteur du système d'information, utilisateur ou administrateur, doit être sensibilisé à l'importance de signaler tout incident réel ou suspecté ; ceci inclut le vol de moyens informatiques ou de supports de données.

Toute infraction susceptible d'implications juridiques fera l'objet d'un dépôt de plainte auprès des autorités compétentes.

10.4. Plan de reprise d'activité

noesya dispose d'un Plan de Reprise d'Activité (PRA) spécifique, disponible publiquement sur son site de gouvernance (https://gouvernance.noesya.coop).

Ce plan doit permettre, dans un premier temps, de maintenir en mode dégradé les activités critiques, puis de récupérer et de restaurer toutes les fonctionnalités du système d'information.

11. Révisions

1.0 Date of change: 25/08/2025 - Responsible: Technical team - Summary of Change: Initial release