1/
La politique de sécurité des systèmes d'information est un plan d'action défini pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information

2/
La **PSSI** constitue un document de référence de sécurité du système d'information (SSI). Celle-ci est là pour définir les objectifs à atteindre, les acteurs associés ainsi que les moyens accordés pour parvenir aux cibles.

3/
Oui dans l'entreprise, elle est rédigée suivant son contexte, on doit cependant la mettre à jour.

4/
Les derniers mois ont été marqués par une **croissance inquiétante des cyberattaques**, et par leur niveau de professionnalisation de plus en plus élevé.
À titre d'illustration, des experts de l'ANSSI ont constaté que le nombre d'intrusions critiques dans les organisations françaises a augmenté de 37 % entre 2020 et 2021 (786 en 2020 contre 1082 en 2021).
Cette hausse s'explique à la fois par :

- l'**évolution et l'amélioration constante des aptitudes des acteurs malveillants** ;
- les **multiples opportunités** offertes par le développement de la transformation digitale des organisations et le rôle de plus en plus important qu'y jouent les systèmes d'information. Ce qui va souvent de pair avec des pratiques (involontairement) dangereuses de la part des collaborateurs…

D'où l'intérêt de mettre en place une PSSI, tant elle offre aux entreprises les clés pour maintenir un **bon niveau de sécurité** pour leurs systèmes d'information.

5/
1 Gérer les responsabilités
Vous l'aurez compris, la sécurité des systèmes d'information revêt une dimension holistique.
Par conséquent, si la PSSI est impulsée par la direction et le **responsable de la sécurité du système d'information**, elle implique également l'intervention d'autres acteurs, à commencer par les directions métiers qui ont un important rôle opérationnel à jouer.
De ce fait, à chaque règle de sécurité, le responsable SI est tenu de déterminer toutes ces parties prenantes concernées et le patrimoine à protéger associé.

2 Déterminer les besoins en ressources
À l'instar de n'importe quelle gestion de projet, il convient par la suite de caractériser les **ressources** que l'exécution du plan d'action va mobiliser, qu'il s'agisse de ressources :

- humaines,
- matérielles,
- ou logicielles.

3 Prioriser les règles de sécurité et les planifier
Comme vous ne pouvez pas tout mener de front, **priorisez les règles de sécurité** à mettre en œuvre, puis **planifiez** le tout dans le temps, notamment à l'aide de jalons.
Sur quels critères hiérarchiser ces règles ? Divers éléments peuvent être pris en compte :

- le degré d'urgence,
- le nombre de ressources que nécessite l'exécution de la règle,`
- la facilité de déploiement, etc.

4 S’améliorer en continu
Il ne s’agit pas d’une étape à proprement parler, mais votre plan opérationnel (tout comme votre PSSI d’ailleurs) doit s’inscrire dans une **démarche d’amélioration continue**, et ne pas rester figé dans le temps.
Afin d’accompagner au mieux l’évolution de votre organisation, mais aussi celle des risques cyber, on vous suggère de remettre régulièrement en question vos choix et dispositions, puis d’apporter des actions correctives.

6/
Les règles contenues dans une PSSI puisent leur légitimité dans les lois, les réglementations, les normes et les recommandations émanant d'instances internationales, nationales ou professionnelles. Elles trouvent également leur justification dans les composantes de la culture de l'organisme comme les traditions, les habitudes ou les règlements internes.

7/
La validation successive des différentes phases vise à faciliter l’implication de la DSI et l’adhésion de tous les intervenants.
Cette étape consiste à vérifier :
- la cohérence des règles énoncées,
- l’exhaustivité de la couverture des risques jugés comme significatifs,
- la traduction complète de l’ensemble des principes et règles, jugés pertinents pour l’organisme et énoncés dans le référentiel présenté en annexe au présent document,
- l’applicabilité des exigences et règles en fonction des pratiques en vigueur au sein de l’organisme.

Enfin, cette étape de revue peut également conduire à réaliser une normalisation, voir une simplification des éléments énoncés dans la politique, notamment dans un document de synthèse qui permettra une meilleure implication de la hiérarchie.

8/
La PSSI doit être régulièrement mise à jour pour suivre l'évolution des technologies, des menaces et des contraintes de l'entreprise. Elle doit être communiquée et comprise par l'ensemble du personnel afin de promouvoir la sécurité de l'information et les bonnes pratiques à adopter.

9/
En amont oui, car une PSSI informatique induit de dresser un **état des lieux des risques** qui planent sur l’organisation. Le document doit donc faire mention :

- de ces différentes menaces,
- de leur degré de criticité,
- du patrimoine qu’elles peuvent impacter,
- des divers scénarios envisagés,
- des actions à mener pour réduire ou éviter ces risques.

Il convient ensuite de mettre en place une **hiérarchisation**, dans l’objectif de prioriser les opérations au moment de passer au plan d’action.

10/
Plan-type d'une PSSI
Le plan qui suit est une proposition de plan générique et compatible avec la démarche méthodologique d'élaboration de politique de sécurité des systèmes d'information.
Ce plan peut être adapté, essentiellement selon les destinataires de la PSSI.
- Partie I - Éléments stratégiques

o Chapitre 1 - Périmètre de la PSSI
Ce chapitre délimite le champ d'application de la PSSI, par exemple en termes de domaines d'activités ou de systèmes d'information.
o Chapitre 2 - Enjeux et orientations stratégiques
Ce chapitre formalise les enjeux liés au périmètre défini dans le chapitre précédent.
o Chapitre 3 - Aspects légaux et réglementaires
Ce chapitre identifie le référentiel légal et réglementaire lié au périmètre de l'étude.
o Chapitre 4 - Échelle de besoins
Ce chapitre présente une échelle de besoins comportant une pondération et des valeurs de référence selon les critères de sécurité choisis, ainsi qu'une liste d'impacts enrichis d'exemples.
o Chapitre 5 - Besoins de sécurité
Ce chapitre expose les besoins de sécurité des domaines d'activité de l'organisme (ou des éléments essentiels), selon l'échelle de besoins présentée dans le chapitre précédent.
o Chapitre 6 – Origines des menaces
Ce chapitre décrit l'ensemble des origines de menaces retenues et non retenues pour le périmètre de l'étude, avec des justifications.

- Partie II - Règles de sécurité
Ce chapitre présente l'ensemble des règles de sécurité classées par thème.
Ces règles sont déclinées des principes de sécurité.

11/
Face aux risques encourus, et dans le contexte fonctionnel et organisationnel propre à l'organisme, il convient d'identifier ce qui doit être protégé, de quantifier l'enjeu correspondant, de formuler des objectifs de sécurité et d'identifier, 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).**

12/
Démarche projet claire et diffusée à tous les acteurs ; - Equipes informatiques impliquées et sensibilisées.

13/
- Répondre aux exigences des normes ISO et l'ANSSI
- Utiliser les bons outils pour piloter la PSSI
- Choisir les bons indicateurs

14/
L'dentification des origines des menaces
Objectif : Cette tâche consiste à identifier et caractériser les origines des menaces qui pèsent sur le périmètre de la PSSI. Ces origines de menaces (éléments menaçants et méthodes d'attaque) seront utiles dans l'élaboration des règles de sécurité et dans toute étude de sécurité dans le périmètre de la PSSI afin d'identifier des objectifs de sécurité d'un système particulier.