POLITIQUE DE SÉCURITÉ

1. INTRODUCTION

- Le rôle prépondérant et en constante évolution du système d'information au sein des organisations implique de renforcer le **niveau de sécurité des entreprises**.

- Face à la résurgence et la professionnalisation des tentatives d'intrusions malveillantes et d'escroqueries, certains documents tels que des politiques et des procédures doivent être soigneusement élaborés.

- La pièce maitresse qui constitue le principal document de référence en matière de **SSI est la Politique de Sécurité du Système d'Information, plus communément appelée la « PSSI ».**

2. Qu'est-ce qu'une Politique de Sécurité du Système d'Information ?

- **La Politique de Sécurité du Système d'Information** définie l'intégralité de la **stratégie de sécurité informatique** de l'entreprise.

- Elle se traduit par la réalisation **d'un document** qui regroupe l'ensemble des **règles de sécurité** à adopter ainsi que le **plan d'actions** ayant pour objectif de **maintenir le niveau de sécurité de l'information** dans l'organisme.

- La PSSI, élaborée « sur-mesure » pour chaque établissement, décrit l'ensemble des **enjeux, des besoins, des contraintes, ainsi que des règles à adopter** propres à chaque structure. Elle doit être validée par la direction et prise en compte par chaque **collaborateur**.

- La PSSI est donc un **document de référence** alliant la stratégie de l'établissement aux acteurs du Système d'Information.

3. Pourquoi mettre en place une Politique de Sécurité du Système d'Information ?

En premier lieu, la démarche de mise en œuvre d'une **PSSI** permet:

- d'entreprendre une évaluation de la maturité de la sécurité de l'organisme,
- d'**identifier les failles et les faiblesses** organisationnelles et techniques afin de prévoir et d'appliquer un **plan d'actions correctives** et des règles associées.

la PSSI est devenue un document de **référence obligatoire** pour tout établissements.

- La Politique de Sécurité du Système d'Information est un document qui doit être pris en compte par chaque collaborateur intervenant dans l'organisme afin qu'il puisse connaître les règles et les enjeux en matière de **sécurité interne et externe** mais aussi des mesures à appliquer en **situation de crise** liée.

- De surcroît définir une PSSI permet également d'évaluer l'importance du rôle que joue le système d'information dans le fonctionnement de l'ensemble des services.

4. Les éléments stratégiques de la PSSI

La Politique de Sécurité du Système d'Information doit comporter **plusieurs grands chapitres**. Ceux-ci pouvant être plus moins détaillés en fonction de l'organisme, de son secteur d'activité et de sa maturité technique et organisationnelle.

- **Le domaine d'application de la PSSI**

Il est nécessaire de clairement **identifier le cadre de la mise en œuvre de la PSSI**. Est-elle applicable à l'ensemble du système d'information de l'organisme ? Est-elle applicable à l'extérieur de l'entreprise ?

- **Les responsabilités de la PSSI** :

Le domaine d'application défini, il est important de connaître le responsable du document, c'est-à-dire **la personne en charge de la définition de son contenu** et à qui est-elle destinée (collaborateurs, prestataires…).

- **Les documents associés** :

Une PSSI n'est rarement constitué que d'un seul document et repose la plupart du temps sur des annexes (**politique de cryptographie, normes, règlement**…) qu'il est indispensable de de référer.

- **Les enjeux internes, externes** :

Pourquoi une politique est-elle mise en œuvre ? Chaque document doit avoir un objectif, un sens. Ainsi, les « enjeux », qu'ils soient internes ou externes doivent être scrupuleusement écrits. Ils sont la base du projet !

- **Les référentiels :**

Au-delà des enjeux, sur **quels cadres réglementaires** se base votre politique de sécurité du système d'information ?

- **La gouvernance** :

Qui est concerné par le **Management de la Sécurité du Système d'Information** au sein de l'organisme ? Il est important d'identifier les fonctions et les rôles spécifiques de chaque intervenant (**Direction, DSI, RSSI, DPO**…) ainsi que des instances mises en place pour **contrôler, auditer et piloter la sécurité de l'information** de l'organisme.

- **Les règles** :

Enfin la PSSI doit spécifier les **principes directeurs et les règles** auxquelles l'entreprise souhaite s'engager **pour garantir la sécurité de son système d'information**. Souvent confondue, la Politique de Sécurité du Système d'Information et la charte informatique sont deux documents différents. **La PSSI fixe le cadre et les règles émises par l'entreprise pour l'ensemble de son système d'information.** La charte informatique quant à elle est un document décrivant ce que le collaborateur à le droit de faire, ce qu'il doit respecter dans le cadre de son quotidien et les sanctions encourues en cas de non respects des règles.

5. Comment mettre en place une Politique de Sécurité du Système d'Information ?

- l'élaboration d'une politique de sécurité nécessite une **approche globale**, portant à la fois sur l'aspect technique tel que la **sécurité logique, la sécurité informatique et la sécurité des réseaux** mais également la **sécurité physique, organisationnelle ainsi que les aspects liés à l'humain**.

- Cette conception ne peut s'effectuer seul. Il s'agit d'un travail d'équipe piloté la plupart du temps par le **Responsable de la Sécurité du Système d'Information (RSSI)** à l'aide de la Direction et de chaque personne composant la gouvernance de la sécurité de l'information (**Directeur du Système d'Information, Délégué à la Protection des Données personnelles, Assistante qualité et gestion des risques**…) mais aussi d'autres collaborateurs tels que certains responsables de services et des ressources humaines.

- Ensemble, le groupe de travail effectuera une **analyse du niveau de maturité SSI** permettra de **définir le périmètre de la politique de sécurité ainsi que ses objectifs**.

- Ensuite, environ 16 domaines devront constituer la Politique de Sécurité du Système d'Information :

Principes organisationnels

1.Politique de sécurité
2.Organisation de la sécurité
3.Gestion des risques SSI
4.Sécurité et cycle de vie
5.Assurance et certification

Principes de mise en œuvre

1.Aspects humains
2.Planification de la continuité des activités
3.Gestion des incidents
4.Sensibilisation et formation
5.Exploitation
6.Aspects physiques et environnementaux

Principes techniques

1.Identification / authentification
2.Contrôle d'accès logique
3.Journalisation
4.Infrastructures de gestion des clés cryptographiques
5.Signaux compromettants

La mise en œuvre d'une Politique de Sécurité du Système d'Information nécessite une méthodologie particulière afin d'impliquer chaque acteur concerné et travailler l'ensemble des domaines nécessaires à sa construction.

Il existe de nombreuses variantes possibles pour une PSSI. Ne soyez donc pas étonné de trouver plusieurs déclinaisons différentes dans la littérature. Pour autant, vous trouverez bien souvent les mêmes grandes lignes. Je vous propose donc un plan type que vous pourrez **adapter** aux besoins particuliers de votre entreprise.

Il est principalement constitué de deux grands axes :

	Titre	Objectifs	Contenu
1	Cadre de la PSSI	Expliciter le rôle de la PSSI pour l'entreprise Déterminer le périmètre d'application de la PSSI	
1.1	Mot de la direction	Montrer l'implication du top management. Expliciter la démarche.	Texte montrant l'importance de la démarche de PSSI pour l'organisme (Proposé par le RSSI et validé par la direction) Prise de conscience des utilisateurs (phase 1)

1.2	Enjeux et champ d'application de la PSSI	Déterminer le champ d'application. Décliner les composants du SI à sécuriser en priorité ainsi que les risques associés.	Objet de la PSSI ;(phase 1) Activités de l'entreprise (métier et support) à intégrer et celles à exclure du périmètre de la PSSI. (phase 1) Bilan des catégories de biens à protéger (phase 2)
2	Contexte	Fixer le périmètre du SI auquel doit s'appliquer la PSSI. Expliciter les enjeux de sécurité de l'entreprise.	

2.1	Enjeux de sécurité	Préciser pourquoi il est important, pour les activités de l'entreprise, de prendre en compte la sécurité.	Les contraintes liées au contexte, aux obligations de la structure, à l'environnement, etc. peuvent également être mentionnées ici si elles sont susceptibles de conditionner les attentes en termes de SSI. (phase 1)
2.2	Cadre légal, réglementaire et obligations contractuelles	Identifier les principaux textes, lois et règlements qui imposent des contraintes vis-à-vis de l'usage du Si de l'entreprise.	Textes législatifs majeurs :

2.3	Principaux risques	Lister les principaux risques pesant sur le SI, hiérarchisés par niveau de risque, afin de définir les priorités de mise en place des mesure de sécurité.	Origine des risques : En s'appuyant sur la méthodologie EBIOS (https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf),vous y listerez les origines humaines délibérées, accidentelles et non humaines. Principaux risques identifiés : Issus d'une analyse de risque et proposée sous forme tabulaire, vous devrez aborder les événement redoutés, les scénarios envisagés le cas échéant, les niveaux de gravité et de vraisemblance. Stratégie de traitement des risques : Pour chaque risque identifié, vous devrez préciser l'option de stratégie macroscopique choisi (réduction, transfert, évitement, maintien). Tout cela s'effectue en phase 3.

3	Exigences et règles de sécurité	Énoncer les exigences et mesures prises en compte pour limiter les risques	Regroupées par thématiques (au sens ISO 27002 du terme que l'on verra), les exigences de sécurité applicables au périmètre de l'entreprise et les mesures mises en oeuvre pour les amoindrir.
4	Annexes	Attacher au document des éléments particuliers	Responsable sécurité de l'entreprise Glossaire Matrice de la couverture exigences / risques Phase 4

6. Les atouts de la PSSI ?

- La sécurité est souvent perçue comme une contrainte paralysant et anesthésiant les processus d'une société. En positionnant d'emblée la PSSI au cœur de tout processus tel le maitre d'arme de l'établissement, la direction pourra combattre cette idée fausse et faire évoluer les postures et les mentalités

- Lorsqu'il s'agit de gestion des risques, les retours sont difficiles à déterminer, accordons nous à dire que la PSSI n'empêchera pas l'erreur humaine ou l'attaque, en revanche si elle est bien élaborée, elle préviendra l'incident ou en limitera les conséquences, en indiquant clairement aux collaborateurs la marche à suivre pour une reprise rapide de l'activité rapide. Les temps d'indisponibilité seront réduits et les risques seront traités grâce à des procédures permettant de réagir rapidement.

- La PSSI fait partie d'un processus d'amélioration continue, lorsqu'un collaborateur impliqué dans la sécurité informatique quitte l'entreprise, la méthodologie et les outils qu'il ou elle utilisaient sont décrits en détail, pour une meilleure transmission de l'information, cette amélioration permet une véritable pérennité pour l'établissement qui en bénéficie.
- Se doter d'une PSSI permet également de renforcer la confiance des utilisateurs et des partenaires, et de respecter les aspects réglementaires.

En résumé :

•une **politique de sécurité des systèmes d'information (PSSI)** reflète la **vision stratégique** de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI) et de gestion de risques SSI. Elle décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme;

•Concrètement, on y trouve :

- la définition des **enjeux** d'une PSSI au regard de l'entreprise, son champ d'application et un **inventaire** des biens (physiques mais aussi organisationnels) à protéger,
- une **analyse** du **contexte réglementaire** de l'entreprise et des **risques** qui pèsent sur le SI,
- la déclinaison des enjeux précédents en **exigences** et **mesures de sécurité**.