PLAN DE SECURITE DES SYSTEMES D’INFORMATION (PSSI)

V 1.0 - 27/08/24

Politique de sécurité et approbation

Créé par	Téléphone	Email	Date	Signature
RSSI	**01.02.03.04**	**rssi@spartan.com**	**27/08/2024**	***RSSI***
Approuvé par			**Date**	**Signature**
Direction	**01.02.03.01**	**direction@spartan.com**		

Suivi des versions

Version	Description	Politique de sécurité #	Date de révision	Date de relecture	Révisé par (Nom + Prénom + Fonction)
1.0	**Version initiale**				

Exigences de conformité

Règle de conformité	Description
ISO 27002	**- Gestion des risques : Identification et évaluation des risques.** **Sécurité physique et environnementale : Protection des infrastructures physiques.** **- Gestion des accès : Contrôles d'accès aux systèmes et aux données.** **- Cryptographie : Méthodes de chiffrement pour protéger les données.** **- Gestion des incidents : Processus de réponse aux incidents de sécurité.**

Table des matières

Politique de sécurité et approbation 2
Suivi des versions 2
Exigences de conformité 2
Table des matières 3
1. Introduction 4
1.1 Objectif du PSSI 4
1.2 Périmètre d'application 4
1.3 Cadre réglementaire et normatif 4
1.4 Responsabilités et gouvernance 5
2. Politique de sécurité de l'information 6
2.1 Principes généraux 6
2.2 Classification de l'information 6
2.3 Gestion des risques 6
3. Contrôles de sécurité techniques 7
3.1 Gestion des accès 7
3.2 Protection des données 7
3.3 Sécurité des réseaux 8
3.4 Sécurité des applications 8
3.5 Surveillance et audit 9
4. Mesures organisationnelles 9
4.1 Sensibilisation et formation 9
4.2 Gestion des incidents 9
4.3 Gestion des changements 10
4.4 Conformité et contrôle interne 10
5. Annexes 11
5.1 Glossaire des termes techniques 11
5.2 Références 11
5.3 Annexe : Organisation Opérationnelle de l'Équipe Blue Team 12
6. Conclusion 12
6.1 Engagement de la direction 12
6.2 Révision et mise à jour du PSSI 12

1. Introduction

1.1 Objectif du PSSI

La Politique de Sécurité des Systèmes d'Information (PSSI) vise à définir les mesures, les contrôles, et les procédures nécessaires pour protéger les actifs informationnels de l'organisation. En tant que fournisseur de services SaaS en ligne, l'organisation doit garantir la confidentialité, l'intégrité et la disponibilité des informations qu'elle gère. Le PSSI est conçu pour prévenir les menaces internes et externes, assurer la conformité avec les régulations applicables, et minimiser les interruptions de service.

1.2 Périmètre d'application

Ce PSSI s'applique à tous les composants du système d'information, y compris mais sans s'y limiter :

- **Serveurs de production** : Hébergent les applications SaaS, les bases de données critiques, et les services clients.
- **Réseaux internes et externes** : Incluent les réseaux de production, les réseaux de test, les réseaux de gestion, et les réseaux publics/privés.
- **Applications SaaS** : Logiciels déployés et accessibles via le cloud, utilisés par les clients de l'organisation.
- **Environnements Active Directory (AD)** : Utilisés pour la gestion des identités et des accès, et pour la configuration des politiques de sécurité.
- **Bases de données** : Stockent des informations critiques, y compris des données clients sensibles.
- **Utilisateurs internes** : Employés de l'organisation ayant accès aux systèmes et données.
- **Prestataires externes** : Fournisseurs de services externalisés, tels que les services de SOC (Security Operations Center) et de gestion des incidents.

1.3 Cadre réglementaire et normatif

Le PSSI s'appuie sur plusieurs normes et régulations internationales et européennes :

- **ISO 27001** : Norme de référence pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI). Cette norme guide l'organisation dans l'identification des risques et la mise en œuvre des contrôles de sécurité.

- **ISO 27002** : Guide pratique fournissant des recommandations pour la gestion des risques, la mise en œuvre de contrôles techniques et organisationnels, et l'amélioration continue des pratiques de sécurité.

- **ISO 27005** : Norme spécifiquement dédiée à la gestion des risques en matière de sécurité de l'information. Elle permet une évaluation systématique des menaces et des vulnérabilités pour assurer une protection efficace des informations.

- **RGPD (Règlement Général sur la Protection des Données)** : Cette régulation européenne impose des exigences strictes en matière de protection des données personnelles. L'organisation doit se conformer aux principes de transparence, de confidentialité, et de protection des droits des personnes concernées.

- **Directive NIS (Network and Information Systems Directive)** : Cette directive européenne impose des exigences de sécurité spécifiques aux opérateurs de services essentiels et aux fournisseurs de services numériques, pour renforcer la résilience des infrastructures critiques contre les cyberattaques.

1.4 Responsabilités et gouvernance

La gouvernance de la sécurité de l'information est assurée par une équipe dédiée, avec des responsabilités bien définies :

- **Responsable de la sécurité des systèmes d'information (RSSI)** : Supervise la mise en œuvre et l'évolution du PSSI. Il est responsable de l'évaluation des risques, de la définition des politiques de sécurité, et de la coordination des initiatives de sécurité à travers l'organisation.

- **Ingénieur/s en sécurité :**

    - **des systèmes (Windows, AD, Linux)** : Chargé de sécuriser les environnements système, y compris les serveurs et les plateformes AD. Ils sont responsables de la gestion des correctifs, de la configuration des politiques de sécurité, et de la surveillance des activités suspectes sur les systèmes.

    - **du réseau** : Assure la protection des réseaux internes et externes. Ils mettent en place des contrôles d'accès réseau, gèrent les pare-feux, les VPN, et les dispositifs IDS/IPS, et sont responsables de la segmentation du réseau pour isoler les différentes zones de sécurité.

    - **des applications** : Garantis que les applications SaaS développées ou utilisées par l'organisation respectent les normes de sécurité les plus strictes. Ils sont responsables des tests de sécurité, de la correction des vulnérabilités applicatives, et de l'intégration des pratiques de développement sécurisé (DevSecOps).

- **Prestataires externes (SOC, Incident Response, Threat Hunting)** : Fournissent des services spécialisés, notamment la surveillance continue des menaces, la

gestion des incidents de sécurité, et l'analyse des cybermenaces avancées. Ils travaillent en étroite collaboration avec l'équipe interne pour assurer une réponse rapide et coordonnée aux incidents.

---

2. Politique de sécurité de l'information

2.1 Principes généraux

Les principes de sécurité de l'information appliqués par l'organisation reposent sur les trois piliers suivants :

- **Confidentialité** : Assurer que seules les personnes autorisées peuvent accéder aux informations sensibles. Cela inclut l'utilisation de méthodes d'authentification robuste, le chiffrement des données, et la gestion stricte des accès.
- **Intégrité** : Garantir que les données ne sont ni altérées ni corrompues de manière non autorisée. Les mécanismes de contrôle d'intégrité, tels que les hachages et les signatures numériques, sont utilisés pour vérifier l'exactitude et la cohérence des informations.
- **Disponibilité** : S'assurer que les systèmes et les informations sont disponibles et accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin. Des mesures de redondance, des sauvegardes régulières, et des plans de reprise après sinistre (PRA) sont en place pour minimiser les interruptions de service.

2.2 Classification de l'information

La classification des informations est essentielle pour déterminer le niveau de protection requis. L'organisation a défini les niveaux de classification suivants :

- **Public** : Informations destinées à être partagées avec le public ou les clients. Aucune restriction particulière n'est appliquée à ces informations, mais elles doivent être vérifiées avant leur diffusion.
- **Interne** : Informations utilisées en interne, dont la divulgation non autorisée pourrait nuire aux opérations de l'organisation. Ces informations doivent être protégées par des contrôles d'accès et des protocoles de confidentialité adaptés.
- **Confidentiel** : Informations sensibles, telles que les données clients, les secrets commerciaux, et les informations financières, dont la divulgation non autorisée pourrait avoir des conséquences graves pour l'organisation. Ces informations doivent être strictement contrôlées, avec un accès limité aux personnes ayant un besoin légitime.

2.3 Gestion des risques

La gestion des risques est un processus continu qui comprend l'identification, l'évaluation, et le traitement des risques associés à la sécurité de l'information. L'organisation suit les étapes suivantes :

- **Identification des menaces** : Identifier les menaces potentielles, qu'elles soient internes (ex. : erreurs humaines, accès non autorisés) ou externes (ex. : cyberattaques, catastrophes naturelles).
- **Évaluation des vulnérabilités** : Analyser les systèmes, les réseaux, et les processus pour détecter les vulnérabilités susceptibles d'être exploitées par les menaces identifiées.
- **Évaluation des impacts** : Estimer les conséquences potentielles d'une exploitation des vulnérabilités, en tenant compte des impacts financiers, opérationnels, juridiques, et réputationnels.
- **Traitement des risques** : Mettre en place des mesures pour réduire les risques à un niveau acceptable. Cela peut inclure l'application de correctifs, l'amélioration des contrôles de sécurité, ou la mise en place de plans de continuité d'activité.

---

3. Contrôles de sécurité techniques

3.1 Gestion des accès

La gestion des accès est un élément clé de la sécurité de l'information. L'organisation met en œuvre les contrôles suivants :

- **Authentification sécurisée** : L'accès aux systèmes critiques est protégé par des mécanismes d'authentification multi-facteurs (MFA). Toutes les connexions sont sécurisées via HTTPS/TLS pour protéger les informations d'authentification en transit.
- **Politiques de mots de passe** : Les utilisateurs doivent créer des mots de passe forts, conformes aux exigences de longueur, de complexité telles que des phrases de pass. Les mots de passe sont stockés de manière sécurisée, hachés avec des algorithmes robustes tels que bcrypt.
- **Contrôles d'accès basés sur les rôles (RBAC)** : L'accès aux informations et aux systèmes est accordé en fonction des rôles et des responsabilités des utilisateurs, conformément au principe du moindre privilège. Les permissions sont régulièrement révisées et ajustées en fonction des changements de rôles ou des départs.

3.2 Protection des données

La protection des données est assurée par un ensemble de mesures techniques et organisationnelles :

- **Chiffrement des données** : Toutes les données sensibles sont chiffrées, tant en transit (via TLS) qu'au repos (via AES-256). Les clés de chiffrement sont gérées de manière sécurisée, avec une rotation régulière et des sauvegardes chiffrées.
- **Sauvegardes régulières** : Des sauvegardes complètes et incrémentielles des données critiques sont effectuées régulièrement. Ces sauvegardes sont stockées sur un serveur dédié, isolé du reste de l'infrastructure, et sont régulièrement testées pour assurer leur intégrité et leur disponibilité.
- **Contrôle d'accès aux bases de données** : L'accès aux bases de données est limité aux utilisateurs autorisés, en appliquant le principe du moindre privilège. Les logs d'accès sont surveillés pour détecter toute activité suspecte.

3.3 Sécurité des réseaux

La sécurité des réseaux est assurée par une combinaison de contrôles techniques et de bonnes pratiques :

- **Migration de Samba vers NetBIOS** : Pour renforcer la sécurité des connexions réseau, la migration de Samba vers NetBIOS est prévue. Cette migration sera planifiée avec soin, avec un déploiement en environnement de test pour minimiser les risques et les interruptions de service.
- **Pare-feux et segmentation du réseau** : Les réseaux sont protégés par des pare-feux configurés pour contrôler le trafic entrant et sortant. La segmentation du réseau est mise en place pour isoler les environnements de production, de test, et de gestion, réduisant ainsi les risques de compromission transversale.
- **Protection des serveurs** : Les serveurs exposés au public sont placés segmentés dans un environnement virtulaisé et protégés par un WAF (Web Application Firewall) pour filtrer les attaques applicatives et renforcer la sécurité des services web.

3.4 Sécurité des applications

Les applications développées ou utilisées par l'organisation doivent respecter des standards élevés de sécurité :

- **Développement sécurisé (DevSecOps)** : Les pratiques de développement sécurisé sont intégrées dès les premières étapes du cycle de vie du développement logiciel (SDLC). Cela inclut des tests de sécurité automatisés, la revue de code, et l'intégration continue (CI/CD) avec des contrôles de sécurité.

- **Filtrage des téléchargements** : Les fichiers téléchargés via les applications sont soumis à un filtrage strict basé sur leur type, leur taille, et leur extension, pour prévenir les risques d'infection par des malwares ou des injections (SQL ou autres).
- **Gestion des patchs** : Tous les logiciels utilisés par l'organisation sont régulièrement mis à jour. Les mises à jour critiques sont déployées en environnement de test et déployées durant la fenêtre de maintenance (2h-4h du matin) pour minimiser l'impact sur les opérations.

3.5 Surveillance et audit

La surveillance continue et les audits réguliers sont essentiels pour détecter et corriger rapidement les failles de sécurité :

- **Monitoring de la sécurité** : Le monitoring des systèmes critiques est assuré par une suite d'outils et surveillé en continu par des analystes SOC externes. Les alertes sont configurées pour détecter les comportements anormaux, les intrusions, et les performances dégradées.
- **Fréquence des audits** : Un audit de sécurité est réalisé au moins une fois par an, avec la possibilité d'audits supplémentaires en fonction des critères définis par le monitoring :
  - Augmentation anormale des alertes de sécurité.
  - Détection d'activités suspectes ou inhabituelles.
  - Incidents de sécurité ayant un impact significatif.
- **Audits internes et externes** : En plus des audits internes, des audits externes sont réalisés par des tiers indépendants pour identifier des opportunités d'amélioration continue.

---

4. Mesures organisationnelles

4.1 Sensibilisation et formation

La sensibilisation et la formation en matière de sécurité sont essentielles pour maintenir un haut niveau de vigilance au sein de l'organisation :

- **Programme de sensibilisation** : Tous les employés reçoivent une formation initiale sur les bonnes pratiques de sécurité, y compris la gestion des mots de passe, la reconnaissance des tentatives de phishing, et les procédures de signalement des incidents. Ce programme est mis à jour régulièrement pour inclure les nouvelles menaces et techniques de protection.

- **Formation continue des équipes de sécurité** : Les membres de l'équipe de sécurité participent à un programme de formation continue pour rester à jour sur les nouvelles vulnérabilités, les technologies émergentes, et les certifications en sécurité. Des ateliers et des simulations de cyberattaques sont également organisés pour renforcer leurs compétences pratiques.

4.2 Gestion des incidents

La gestion des incidents de sécurité suit un processus structuré pour minimiser l'impact sur les opérations et restaurer les services rapidement :

- **Détection des incidents** : Les incidents de sécurité sont détectés par le monitoring continu des systèmes critiques et par les alertes émises par les outils de sécurité. Les employés sont également encouragés à signaler toute activité suspecte via un canal de communication dédié.
- **Réponse aux incidents** : Une équipe dédiée à la réponse aux incidents, incluant des membres internes et des prestataires externes, est activée dès qu'un incident est confirmé. L'équipe suit un plan d'intervention prédéfini, incluant l'identification de la cause, la mise en œuvre de contre-mesures, et la communication avec les parties prenantes.
- **Récupération et analyse post-incident** : Après la résolution de l'incident, une analyse approfondie est réalisée pour comprendre les causes sous-jacentes et mettre en place des mesures correctives. Un rapport d'incident est préparé, documentant les actions entreprises, les leçons apprises, et les améliorations nécessaires pour prévenir de futurs incidents.

4.3 Gestion des changements

La gestion des changements est cruciale pour éviter les interruptions de service et maintenir la sécurité des systèmes :

- **Processus de gestion des changements** : Tout changement dans l'infrastructure ou les systèmes d'information doit être soumis à un processus d'approbation formel. Ce processus comprend une évaluation des impacts, des tests en environnement de staging, et une validation finale par les responsables concernés avant le déploiement en production.
- **Fenêtre de maintenance** : Les changements sont déployés pendant une fenêtre de maintenance dédiée, de 2h à 4h du matin, pour minimiser les interruptions de service. Les utilisateurs sont informés à l'avance des éventuelles perturbations.

4.4 Conformité et contrôle interne

Le respect des politiques de sécurité et des régulations est assuré par un système de contrôle interne rigoureux :

- **Audits de conformité** : Des audits internes sont réalisés régulièrement pour s'assurer que les pratiques de sécurité respectent les normes ISO 27001, ISO 27002, et ISO 27005. Ces audits incluent la vérification des contrôles d'accès, la protection des données, et la gestion des incidents.

- **Actions correctives** : En cas de non-conformité, des actions correctives sont immédiatement mises en place, avec un suivi régulier pour s'assurer de leur efficacité. Les écarts identifiés lors des audits externes sont également traités en priorité pour maintenir la conformité réglementaire.

---

5. Annexes

5.1 Glossaire des termes techniques

- **Authentification Multi-Facteurs (MFA)** : Méthode de contrôle d'accès dans laquelle l'utilisateur doit fournir plusieurs éléments d'identification distincts pour vérifier son identité.

- **Chiffrement AES-256** : Algorithme de chiffrement symétrique qui utilise une clé de 256 bits pour sécuriser les données.

- **Pare-feu (Firewall)** : Système de sécurité réseau qui contrôle le trafic entrant et sortant en fonction de règles de sécurité prédéfinies.

- **Web Application Firewall (WAF)** : Dispositif de sécurité qui protège les applications web contre diverses menaces, telles que les injections SQL, les scripts intersites (XSS), et d'autres vulnérabilités applicatives.

- **RBAC (Role-Based Access Control)** : Modèle de gestion des accès où les permissions sont accordées en fonction du rôle de l'utilisateur dans l'organisation.

- **SOC (Security Operations Center)** : Équipe de sécurité qui surveille en continu les événements de sécurité, détecte les menaces, et répond aux incidents.

- **WSUS (Windows Server Update Services)** : Outil de gestion des mises à jour développé par Microsoft, permettant aux administrateurs de gérer la distribution des mises à jour pour les produits Microsoft dans un environnement d'entreprise.

5.2 Références

Normes et régulations :

- ISO/IEC 27001:2013 – Information security management systems.
- ISO/IEC 27002:2013 – Code of practice for information security controls.
- ISO/IEC 27005:2018 – Information security risk management.

- Règlement Général sur la Protection des Données (RGPD).
- Directive NIS (Network and Information Systems Directive).

Littérature complémentaire :

- NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations.
- OWASP Top Ten – Liste des dix principales vulnérabilités de sécurité des applications web.
- SANS Institute Reading Room – Collection de documents sur les meilleures pratiques en sécurité de l'information.

5.3 Annexe : Organisation Opérationnelle de l'Équipe Blue Team

Cette annexe détaille l'organisation et les responsabilités de l'équipe Blue Team, chargée de la défense des systèmes d'information de l'organisation. Élaborée dans le cadre de l'audit de l'infrastructure, elle présente la répartition des rôles et les tâches quotidiennes nécessaires pour maintenir la sécurité, détecter les menaces, et répondre efficacement aux incidents. Ce document illustre la mise en œuvre pratique des politiques de sécurité définies dans ce PSSI, assurant ainsi une défense coordonnée et proactive contre les menaces cybernétiques.

---

6. Conclusion

6.1 Engagement de la direction

La direction de l'organisation réaffirme son engagement à soutenir la mise en œuvre de cette Politique de Sécurité des Systèmes d'Information. Les ressources nécessaires, tant financières qu'humaines, seront allouées pour garantir la protection continue des informations et la résilience des systèmes. La direction s'engage également à promouvoir une culture de la sécurité au sein de l'organisation, où chaque employé est conscient de son rôle dans la protection des actifs informationnels.

6.2 Révision et mise à jour du PSSI

Ce PSSI sera révisé deux fois par an pour tenir compte des nouvelles menaces, des évolutions technologiques, et des changements dans le cadre réglementaire. Les audits de sécurité seront réalisés au moins une fois par an, avec des audits supplémentaires déclenchés selon les critères définis par le monitoring. La mise à jour du PSSI sera effectuée en collaboration avec toutes les parties prenantes, et les modifications seront communiquées à l'ensemble du personnel pour assurer une mise en œuvre cohérente.

Annexe :

Organisation Opérationnelle de l'Équipe Blue Team