Politique de Sécurité des Systèmes d'Information (PSSI)

INTRODUCTION

Dans un contexte de transformation numérique accrue et de multiplication des menaces cyber, la sécurité des systèmes d'information constitue un enjeu stratégique majeur pour DataSecure Inc., entreprise spécialisée dans la gestion de données sensibles pour ses clients.

La confiance accordée par les clients, partenaires et autorités de régulation repose sur la capacité de DataSecure Inc. à garantir :

- la confidentialité,
- l'intégrité,
- la disponibilité,
- et la traçabilité des informations qu'elle traite.

La présente Politique de Sécurité des Systèmes d'Information (PSSI) définit le cadre stratégique, organisationnel et opérationnel permettant de protéger les actifs informationnels de l'entreprise et de maîtriser les risques identifiés, notamment ceux liés au vol de données et à la non-conformité réglementaire.

Cette PSSI s'inscrit dans le cadre du Système de Management de la Sécurité de l'Information (SMSI) de DataSecure Inc., fondé sur une analyse de risques réalisée selon la méthodologie EBIOS Risk Manager. Elle est alignée sur les normes ISO/IEC 27001 et ISO/IEC 27002, ainsi que sur les exigences réglementaires applicables, notamment DORA, NIS2, SOC 2 et les obligations légales en vigueur.

La PSSI a vocation à :

- définir les objectifs et principes de sécurité,
- préciser les rôles et responsabilités des acteurs,
- établir les règles de sécurité applicables à l'ensemble du périmètre,
- servir de référence commune pour toutes les parties prenantes.

Elle s'applique à l'ensemble des collaborateurs, prestataires et partenaires intervenant sur le périmètre des systèmes d'information de DataSecure Inc.

PARTIE I - ÉLEMENTS STRATEGIQUES

Chapitre 1 - Périmètre de la PSSI

1.1 Champ d'application organisationnel

La présente Politique de Sécurité des Systèmes d'Information (PSSI) s'applique à l'ensemble de DataSecure Inc., incluant :

- la direction générale,
- les directions métiers,
- la DSI et les équipes techniques,
- la fonction sécurité (RSSI),
- la fonction conformité et juridique,
- l'ensemble des collaborateurs, internes et externes,
- les prestataires et sous-traitants accédant au SI.

1.2 Champ d'application technique

La PSSI couvre l'ensemble des systèmes d'information contribuant à la gestion de données sensibles clients, notamment :

- infrastructures de stockage et de traitement des données,
- environnements cloud et datacenters,
- applications métiers et plateformes clients,
- réseaux internes et interconnexions,
- outils de sécurité (IAM, SIEM, DLP, SOC),
- dispositifs de journalisation et de supervision.

1.3 Système de Sécurité de l'Information (SSI)

Le SSI de DataSecure Inc. regroupe :

- l'ensemble des moyens humains, organisationnels, techniques et contractuels
- destinés à assurer la confidentialité, l'intégrité, la disponibilité, la traçabilité et la conformité des informations.

1.4 Système de Management de la Sécurité de l'Information (SMSI)

La PSSI constitue un document socle du SMSI, conforme à la norme ISO/IEC 27001, et s'inscrit dans une démarche d'amélioration continue (PDCA).

Chapitre 2 - Enjeux et orientations stratégiques

2.1 Enjeux majeurs

Les principaux enjeux identifiés pour DataSecure Inc. sont :

- protection des données sensibles clients,
- maintien de la confiance des clients et partenaires,
- conformité aux exigences réglementaires et normatives,
- continuité des activités,
- préservation de la réputation et de la valeur de l'entreprise.

2.2 Orientations stratégiques de sécurité

La stratégie de sécurité repose sur les axes suivants :

- réduction prioritaire des risques critiques identifiés (vol de données, non-conformité),
- intégration de la sécurité dès la conception (security by design),
- gouvernance forte de la sécurité pilotée par la direction,
- maîtrise des risques liés aux tiers,
- amélioration continue du niveau de maturité SSI.

Chapitre 3 - Aspects légaux et réglementaires

3.1 Référentiels applicables

DataSecure Inc. est soumise notamment aux référentiels suivants :

- ISO/IEC 27001 & 27002 – management et contrôles de sécurité,
- DORA – résilience opérationnelle numérique,
- NIS2 – sécurité des réseaux et systèmes d'information,
- SOC 2 – critères de sécurité, disponibilité, confidentialité,
- RGPD – protection des données personnelles,
- obligations contractuelles clients et partenaires.

3.2 Objectif de conformité

L'objectif est de :

- démontrer la conformité,
- produire des preuves auditées,
- assurer une veille réglementaire continue

Chapitre 4 - Échelle de besoins

4.1 Critères de sécurité retenus

- Confidentialité
- Intégrité
- Disponibilité
- Traçabilité
- Conformité

4.2 Échelle de pondération

Niveau	Valeur	Description
Faible	1	Impact limité, réversible
Moyen	2	Impact significatif mais maîtrisable
Élevé	3	Impact sérieux sur l'activité
Critique	4	Impact majeur, systémique

4.3 Exemples d'impacts

- Critique : fuite massive de données clients, sanctions réglementaires majeures.
- Élevé : indisponibilité prolongée d'un service client.
- Moyen : non-conformité documentaire ponctuelle.
- Faible : incident isolé sans impact client.

Chapitre 5 – Besoins de sécurité

Les besoins de sécurité pour DataSecure Inc. sont évalués comme suit :

Critère	Niveau
Confidentialité	Critique
Intégrité	Élevée
Disponibilité	Élevée
Traçabilité	Élevée
Conformité	Critique

Chapitre 6 – Origines des menaces

6.1 Origines retenues

- cybercriminels organisés,
- menaces internes (malveillance, négligence),
- prestataires et tiers,
- erreurs humaines,
- défaillances de gouvernance.

6.2 Origines non retenues

- menaces physiques majeures (hors périmètre),
- conflits étatiques directs (non avérés dans le contexte).

Ces choix sont justifiés par l'analyse de risques EBIOS RM.

PARTIE II - REGLES DE SECURITE

1. Gouvernance et organisation de la sécurité

Règle

La direction de DataSecure Inc. s'engage formellement dans la sécurité de l'information et définit clairement les rôles et responsabilités en matière de SSI.

Contrôles

- 5.1 Politiques de sécurité de l'information
- 5.2 Rôles et responsabilités en matière de sécurité

Processus opérationnel de vérification

- Validation annuelle de la PSSI en comité de direction.
- Désignation formelle du RSSI par note de service.
- Revue annuelle de l'organigramme SSI.

- Vérification par audit interne de l'existence des décisions et comptes rendus.

2. Gestion des risques et conformité

Règle

Les risques de sécurité de l'information sont identifiés, évalués, traités et suivis de manière continue dans le cadre du SMSI.

Contrôles

- 5.4 Gestion des risques de sécurité de l'information
- 5.31 Exigences légales, réglementaires et contractuelles

Processus opérationnel de vérification

- Réalisation d'une analyse de risques EBIOS RM annuelle.
- Tenue d'un registre des risques SSI.
- Suivi trimestriel des plans de traitement.
- Audit interne vérifiant la mise à jour du registre et l'état des actions

3. Gestion des accès et des identités

Règle

Les accès aux systèmes et aux données sont accordés selon le principe du moindre privilège et font l'objet d'un contrôle strict.

Contrôles

- 8.2 Gestion des identités
- 8.3 Gestion des informations d'authentification

Processus opérationnel de vérification

- Processus formalisé de demande, validation et révocation des accès.
- Revue trimestrielle des droits d'accès par les responsables applicatifs.
- Contrôle du déploiement du MFA sur les comptes sensibles.
- Vérification via rapports IAM et journaux d'authentification.

4. Protection des données

Règle

Les données sensibles sont protégées contre toute divulgation, altération ou perte, tout au long de leur cycle de vie.

Contrôles

- 8.10 Suppression de l'information
- 8.24 Utilisation de la cryptographie

Processus opérationnel de vérification

- Classification des données et registre associé.
- Vérification du chiffrement des données au repos et en transit.
- Revue périodique des politiques de rétention et de suppression.
- Tests de conformité via audits techniques et revues d'architecture.

5. Sécurité des opérations et des systèmes

Règle

Les systèmes d'information sont exploités de manière sécurisée, durcis et maintenus à jour afin de réduire les vulnérabilités.

Contrôles

- 8.9 Gestion de la configuration
- 8.8 Gestion des vulnérabilités techniques

Processus opérationnel de vérification

- Mise en place de référentiels de configuration sécurisée.
- Scans de vulnérabilités périodiques.
- Suivi des correctifs dans un outil de gestion des changements.
- Revue mensuelle des rapports de vulnérabilité.

6. Journalisation et surveillance

Règle

Les événements de sécurité sont journalisés, protégés et analysés afin de détecter les incidents et démontrer la conformité.

Contrôles

- 8.15 Journalisation
- 8.16 Surveillance des activités

Processus opérationnel de vérification

- Centralisation des journaux dans un SIEM.
- Définition de cas d'usage de détection.
- Revue quotidienne des alertes de sécurité.
- Vérification lors d'audits de la disponibilité et de l'intégrité des logs.

7. Gestion des incidents de sécurité

Règle

Tout incident de sécurité de l'information est détecté, qualifié, traité et documenté selon un processus formalisé.

Contrôles

- 5.24 Gestion des incidents de sécurité de l'information

Processus opérationnel de vérification

- Existence d'une procédure de gestion des incidents.
- Enregistrement des incidents dans un outil de ticketing.
- Exercices de simulation d'incident annuels.
- Revue post-incident et validation des actions correctives.

8. Sécurité des relations avec les tiers

Règle

Les prestataires et partenaires respectent les exigences de sécurité de DataSecure Inc. et font l'objet d'un suivi régulier.

Contrôles

- 5.19 Sécurité de l'information dans les relations avec les fournisseurs
- 5.21 Gestion de la sécurité des services externalisés

Processus opérationnel de vérification

- Évaluation de sécurité avant contractualisation.
- Clauses contractuelles SSI obligatoires.
- Audits ou questionnaires de sécurité annuels.
- Suivi des écarts et plans de remédiation prestataires.

9. Sensibilisation et formation à la sécurité

Règle

Les collaborateurs sont régulièrement sensibilisés aux enjeux de sécurité de l'information et à leurs responsabilités.

Contrôles

- 6.3 Sensibilisation, éducation et formation à la sécurité

Processus opérationnel de vérification

- Programme annuel de formation SSI.
- Sessions obligatoires pour les nouveaux arrivants.
- Campagnes de phishing simulé.
- Suivi des taux de participation et des résultats.

10. Amélioration continue du SMSI

Règle

Le SMSI est régulièrement évalué afin d'en améliorer l'efficacité et l'adéquation aux risques.

Contrôles

- 5.36 Revue indépendante de la sécurité de l'information

Processus opérationnel de vérification

- Audits internes annuels du SMSI.
- Revues de direction formalisées.
- Suivi des non-conformités et actions correctives.
- Indicateurs SSI présentés périodiquement à la direction.

CONCLUSION

La présente Politique de Sécurité des Systèmes d'Information constitue le socle de référence de la sécurité de l'information au sein de DataSecure Inc. Elle formalise l'engagement de l'entreprise à protéger durablement ses actifs informationnels et à maîtriser les risques cyber auxquels elle est exposée.

La sécurité des systèmes d'information est une responsabilité partagée. Chaque collaborateur, quel que soit son rôle, est tenu de respecter les règles définies par la PSSI et de contribuer activement à la protection des informations et des systèmes.

La Direction Générale de DataSecure Inc. affirme son engagement fort en matière de sécurité de l'information en :

- soutenant le déploiement et le maintien du SMSI,
- allouant les ressources nécessaires,
- acceptant ou arbitrant les risques résiduels identifiés,
- promouvant une culture de sécurité au sein de l'organisation.

La PSSI est un document vivant, soumis à un processus d'amélioration continue. Elle est révisée périodiquement afin de :

- prendre en compte l'évolution des menaces,
- intégrer les changements organisationnels et technologiques,
- répondre aux nouvelles exigences réglementaires,
- améliorer l'efficacité des mesures de sécurité mises en œuvre.

Toute évolution majeure du périmètre, des risques ou du cadre réglementaire donnera lieu à une mise à jour formelle de la PSSI, validée par la Direction Générale.

ANNEXES

A1-ANALYSE DE RISQUE DETAILLEE DE DATASECURE INC

ATELIER 1 – Cadrage et socle de sécurité

L'objectif est de poser un cadre clair, partagé et exploitable pour les ateliers suivants. Je déroule l'atelier de manière structurée.

1. Contexte et objectifs de l'analyse

Contexte métier

DataSecure Inc. fournit des services de :

- stockage,
- traitement,
- sécurisation,
- mise à disposition

de données sensibles appartenant à des clients (potentiellement données personnelles, financières, contractuelles, industrielles).

L'entreprise est donc :

- tiers de confiance,
- fortement exposée réglementairement,
- cible à forte valeur pour les attaquants.

Objectifs de l'analyse de risques

- Identifier et maîtriser les risques majeurs liés :
    - au vol de données
    - à la non-conformité réglementaire

- Protéger :
    - les actifs informationnels critiques,
    - la continuité d'activité,
    - la conformité légale et contractuelle,
    - la réputation de DataSecure Inc.

2. Périmètre de l'étude

Périmètre organisationnel

Inclus :

- Direction générale
- DSI / RSSI
- Équipes d'exploitation IT
- Équipes conformité / juridique
- Prestataires critiques (cloud, infogérance, SOC)

Exclus (à ce stade) :

- Fonctions RH hors SI
- Activités non liées aux données clients

Périmètre technique

Inclus :

- Systèmes de stockage des données clients
- Applications de gestion et d'accès aux données
- Infrastructures cloud / datacenter
- Réseaux internes et d'interconnexion
- Outils de supervision et de sécurité (SIEM, IAM, DLP, etc.)

3. Actifs essentiels

Actifs primaires

- Données sensibles des clients
    - données personnelles
    - données financières
    - données contractuelles
    - données stratégiques

Actifs de support critiques

- Plateformes de stockage
- Applications métiers
- Systèmes d'authentification et de gestion des accès
- Journaux de sécurité et de conformité
- Contrats clients et engagements réglementaires

4. Événements redoutés

Conformément à EBIOS RM, on raisonne en impact métier, pas encore en menaces.

Événement redouté n°1 – Vol de données

Divulgation, exfiltration ou accès non autorisé aux données sensibles des clients.

Impacts potentiels :

- Rupture de confidentialité
- Pertes financières
- Sanctions réglementaires
- Perte de confiance clients
- Atteinte à la réputation

Événement redouté n°2 – Non-conformité réglementaire

Manquement aux obligations DORA, NIS2, SOC 2, ISO 27001/27002.

Impacts potentiels :

- Amendes et sanctions
- Résiliation de contrats
- Interdiction d'opérer certains services
- Dégradation de l'image de marque

5. Critères de sécurité retenus

Pour DataSecure Inc., les critères prioritaires sont :

- Confidentialité : CRITIQUE
- Intégrité : ÉLEVÉE
- Disponibilité : ÉLEVÉE
- Traçabilité / preuve : ÉLEVÉE
- Conformité : CRITIQUE

6. Hypothèses structurantes

- DataSecure Inc. est soumise à des exigences contractuelles strictes.
- Une violation majeure aurait un impact systémique sur l'entreprise.
- Les attaquants peuvent être :
    - externes (cybercriminels),
    - internes (malveillance ou erreur),
    - indirects (prestataires).

ATELIER 2 – SOURCES DE RISQUE

Objectif de l'atelier 2

Identifier et caractériser les sources de risque susceptibles de provoquer les événements redoutés *« Vol de données sensibles clients »*, et pouvant conduire à un manquement réglementaire ou normatif, volontaire ou non.

Matrice de détermination du niveau de menace

MOTIVATION					
1 (faible)	2 (moyen)	3 (élevé)	4(très élevé)		
Critique	Critique	Critique	Critique	4(très élevé)	RESSOURCES
Elevé	Elevé	Elevé	Elevé	3 (élevé)	
Moyen	Elevé	Elevé	Elevé	2 (moyen)	
Faible	Faible	Moyen	Moyen	1 (faible)	

RISQUE 1 : VOL DE DONNÉES

On répond à la question :

Qui pourrait être à l'origine du risque, avec quelles intentions et capacités ?

Source du Risque	Objectif Visé	Motivation	Ressources	Niveau de Menace
Cybercriminels organisés	Exfiltration massive de données clients Revente sur le dark web Extorsion (double extorsion)	4	4	Critique
Interne malveillant	Vol de données à des fins personnelles Représailles Avantage concurrentiel	2 à 3	3	Elevé
Interne négligent	Non intentionnels	1	1 à 2	Elevé

Prestataire compromis	Indirects ou involontaires	1	3	Elevé
Hacktivistes / concurrents	Atteinte à l'image Sabotage Divulgation publique de données	1	2	Moyen

RISQUE 2 : NON-CONFORMITÉ (DORA, NIS2, SOC 2, ISO 27001/27002)

Source du Risque	Objectif Visé	Motivation	Ressources	Niveau de Menace
Gouvernance insuffisante	Non intentionnels	1	4	Critique
Équipe GRC sous-dimensionnée	Charge de travail excessive Manque de compétences spécifiques (DORA, NIS2) Documentation incomplète ou obsolète	1	3	Elevé
Erreurs humaines	Mauvaise application des procédures Non-respect des politiques de sécurité Absence de formation régulière	1	2	Moyen
Prestataires non conformes	Clauses contractuelles insuffisantes Absence d'audit fournisseur Manque de suivi des exigences DORA/NIS2	1	3	Elevé

Évolutions réglementaires	Changements rapides des exigences Retards de mise en conformité Mauvaise veille réglementaire	1	2	Moyen

ATELIER 3 & 4 – SCENARIOS STRATEGIQUES ET OPERATIONNELS

RISQUE 1 – VOL DE DONNÉES

SCÉNARIOS STRATEGIQUES

Scénario stratégique VD-1

Cybercriminels organisés

Narratif
Un groupe cybercriminel cible DataSecure Inc. pour exfiltrer des données clients en vue de revente ou d'extorsion.

Sources de risque

- Cybercriminels organisés

Objectif

- Vol massif de données sensibles

Gravité

- CRITIQUE
    - pertes financières majeures,
    - sanctions réglementaires,
    - perte de clients,
    - atteinte durable à la réputation.

Vraisemblance

- ÉLEVÉE
    - secteur très attractif,
    - exposition permanente,
    - attaques observées dans l'écosystème.

Scénario stratégique VD-2

Interne malveillant

Narratif
Un employé disposant d'accès légitimes extrait des données clients à des fins personnelles.

Sources de risque

- Employé interne malveillant

Gravité

- ÉLEVÉE
    - volume potentiellement important,
    - forte atteinte à la confiance.

Vraisemblance

- MOYENNE
    - dépendante du contexte RH,
    - occurrence plus rare que les attaques externes.

Scénario stratégique VD-3

Prestataire compromis

Narratif
Un prestataire critique est compromis, donnant accès indirect aux données clients.

Sources de risque

- Prestataire / fournisseur IT

Gravité

- CRITIQUE
    - exposition large,
    - responsabilité contractuelle directe.

Vraisemblance

- MOYENNE à ÉLEVÉE
    - dépend de la maturité fournisseur,
    - interconnexions fréquentes.

Synthèse

Scénario	Vraisemblance	Gravité
VD-1 Cybercriminels	ÉLEVÉE	CRITIQUE
VD-2 Interne malveillant	MOYENNE	ÉLEVÉE
VD-3 Prestataire compromis	MOYENNE / ÉLEVÉE	CRITIQUE

SCÉNARIOS OPÉRATIONNELS

Scénario opérationnel VD-O1

Phishing → compromission compte → exfiltration

- Source : cybercriminels
- Mode opératoire :
    - phishing ciblé,
    - vol d'identifiants,
    - accès aux données clients.

Gravité

- CRITIQUE

Vraisemblance

- ÉLEVÉE

- vecteur largement observé.

Scénario opérationnel VD-O2

Mauvaise configuration cloud

- Source : erreur interne / attaquant externe opportuniste
- Mode opératoire :
  - bucket exposé,
  - absence de contrôle d’accès.

Gravité

- CRITIQUE

Vraisemblance

- MOYENNE
  - dépend des processus de revue.

Scénario opérationnel VD-O3

Abus de privilèges internes

- Source : interne malveillant
- Mode opératoire :
  - extraction progressive de données,
  - dissimulation via accès légitime.

Gravité

- ÉLEVÉE

Vraisemblance

- MOYENNE

Synthèse

Scénario opérationnel	Vraisemblance	Gravité
VD-O1 Phishing	ÉLEVÉE	CRITIQUE
VD-O2 Cloud mal configuré	MOYENNE	CRITIQUE
VD-O3 Abus privilèges	MOYENNE	ÉLEVÉE

RISQUE 2 – NON-CONFORMITÉ RÉGLEMENTAIRE

ATELIER 3 – SCÉNARIOS STRATÉGIQUES

Scénario stratégique NC-1

Gouvernance défaillante

Narratif
La direction sous-estime les exigences réglementaires, entraînant des écarts majeurs lors d'un audit.

Gravité

- CRITIQUE

Vraisemblance

- MOYENNE

Scénario stratégique NC-2

Documentation et contrôles insuffisants

Narratif
Les politiques, procédures et preuves de conformité sont incomplètes ou obsolètes.

Gravité

- ÉLEVÉE

Vraisemblance

- ÉLEVÉE

Scénario stratégique NC-3

Prestataire non conforme

Narratif
Un fournisseur critique ne respecte pas les exigences DORA/NIS2, engageant la responsabilité de DataSecure Inc.

Gravité

- CRITIQUE

Vraisemblance

- MOYENNE

Synthèse

Scénario	Vraisemblance	Gravité
NC-1 Gouvernance	MOYENNE	CRITIQUE
NC-2 Documentation	ÉLEVÉE	ÉLEVÉE
NC-3 Prestataire	MOYENNE	CRITIQUE

ATELIER 4 – SCÉNARIOS OPÉRATIONNELS

Scénario opérationnel NC-O1

Absence de journalisation et preuves

- Source : organisation interne
- Impact : incapacité à démontrer la conformité lors d'un audit.

Gravité

- ÉLEVÉE

Vraisemblance

- ÉLEVÉE

Scénario opérationnel NC-O2

Non-respect des exigences DORA (gestion des tiers)

- Source : prestataire
- Impact : sanctions réglementaires.

Gravité

- CRITIQUE

Vraisemblance

- MOYENNE

Scénario opérationnel NC-O3

Veille réglementaire insuffisante

- Source : gouvernance / GRC
- Impact : retard de mise en conformité NIS2.

Gravité

- ÉLEVÉE

Vraisemblance

- MOYENNE

Synthèse

Scénario opérationnel	Vraisemblance	Gravité
NC-O1 Preuves absentes	ÉLEVÉE	ÉLEVÉE
NC-O2 Tiers non conformes	MOYENNE	CRITIQUE
NC-O3 Veille insuffisante	MOYENNE	ÉLEVÉE

ATELIER 5 : TRAITEMENT DES RISQUES

1. Renommage des risques (base de consolidation)

VOL DE DONNES

ID	Description du risque
R1	Cybercriminels organisés – Exfiltration massive de données
R2	Interne malveillant – Abus de privilèges
R3	Prestataire compromis – Accès indirect aux données
R4	Phishing → compromission de compte → vol de données
R5	Mauvaise configuration cloud exposant des données

NON-CONFORMITÉ REGLEMENTAIRE

ID	Description du risque
R6	Gouvernance insuffisante – Non-conformité majeure
R7	Documentation et contrôles incomplets
R8	Prestataire non conforme (DORA / NIS2)
R9	Absence de preuves et journalisation
R10	Absence de preuves et journalisation

4. QUALIFICATION FINALE

Risque	Vraisemblance	Gravité
R1	Élevée	Critique
R2	Moyenne	Élevée
R3	Moyenne / Élevée	Critique
R4	Élevée	Critique
R5	Moyenne	Critique
R6	Moyenne	Critique
R7	Élevée	Élevée
R8	Moyenne	Critique
R9	Élevée	Élevée

R10	Moyenne	Élevée

MATRICE DE RISQUES

Gravité

Vraisemblance

Liste des mesures de sécurité recommandées alignées sur la norme ISO 27002

R1 : Cybercriminels organisés – Exfiltration massive de données

- 8.2.1 Contrôle d'accès strict (principe du moindre privilège, séparation des fonctions)
- 8.3.1 Authentification forte multifactorielle (MFA) sur accès sensibles
- 8.7.1 Protection des communications (chiffrement des données en transit et au repos)
- 12.4.1 Surveillance et détection des incidents (SIEM, IDS/IPS)
- 16.1.1 Plan de gestion des incidents de sécurité et exercices réguliers
- 14.2.3 Renforcement des systèmes (patching rapide, durcissement OS/applications)
- 18.1.4 Sensibilisation régulière au phishing et campagnes anti-hameçonnage
- 15.1.1 Analyse régulière des vulnérabilités et tests d'intrusion

R2 : Interne malveillant – Abus de privilèges

- 8.2.2 Gestion rigoureuse des droits d'accès, revue périodique des privilèges
- 8.3.3 Journalisation et surveillance des accès privilégiés (accountability)
- 9.2.1 Contrôles d'intégrité sur les actions des utilisateurs (alertes sur comportements anormaux)
- 7.2.2 Code de conduite et politique d'utilisation des ressources clairement définie

- 16.1.4 Mécanismes de signalement confidentiel des comportements suspects
- 7.2.3 Formations régulières et sensibilisation aux risques internes

R3 : Prestataire compromis – Accès indirect aux données

- 15.1.2 Sélection rigoureuse des prestataires, clauses contractuelles sur sécurité
- 15.2.1 Surveillance et audit périodique des prestataires
- 8.2.5 Gestion et contrôle des accès des tiers (accès limités, temporaires, révoqués rapidement)
- 13.2.1 Protection des informations échangées avec les tiers (chiffrement, règles de transfert)
- 18.1.3 Sensibilisation des prestataires aux exigences de sécurité
- 12.4.3 Surveillance des activités des tiers sur les systèmes

R4 : Phishing → compromission de compte → vol de données

- 7.2.3 Sensibilisation et formation régulière des utilisateurs au phishing
- 8.3.1 Mise en place de MFA pour tous les accès distants et sensibles
- 12.4.1 Surveillance des tentatives d'accès suspectes
- 18.1.4 Exercices d'hameçonnage simulé (phishing simulation)
- 9.2.2 Détection et blocage des emails malveillants (filtrage anti-spam / anti-phishing)

R5 : Mauvaise configuration cloud exposant des données

- 14.2.2 Normes strictes de configuration et durcissement des environnements cloud
- 12.3.1 Gestion des configurations et gestion des changements contrôlée
- 15.1.1 Analyse régulière des vulnérabilités et audits de sécurité cloud
- 8.2.5 Contrôle d'accès strict aux consoles cloud
- 13.2.1 Chiffrement des données sensibles dans le cloud
- 18.1.2 Formation des équipes techniques cloud aux bonnes pratiques de sécurité

R6 : Gouvernance insuffisante – Non-conformité majeure

- 5.1.1 Engagement de la direction formel et communication claire des responsabilités
- 6.1.1 Politique de sécurité de l'information documentée et diffusée
- 6.1.2 Planification et pilotage du SMSI avec objectifs mesurables
- 7.1.2 Gestion des compétences et formations pour la gouvernance et conformité
- 18.1.1 Surveillance réglementaire et veille juridique continue
- 16.1.1 Audit interne régulier du SMSI

R7 : Documentation et contrôles incomplets

- 6.2.1 Mise à jour régulière des politiques et procédures
- 7.5.3 Contrôle documentaire et gestion des versions
- 12.4.1 Suivi et journalisation des modifications des systèmes
- 14.2.1 Gestion rigoureuse des changements (change management)
- 7.2.1 Sensibilisation à l'importance des procédures documentées

R8 : Prestataire non conforme (DORA / NIS2)

- 15.1.3 Clauses contractuelles détaillées sur la conformité réglementaire
- 15.2.2 Évaluations régulières de la conformité des prestataires
- 15.2.3 Plans de remédiation et suivi des écarts avec prestataires
- 13.2.1 Confidentialité et intégrité des échanges avec prestataires
- 18.1.3 Formation et sensibilisation aux exigences DORA / NIS2

R9 : Absence de preuves et journalisation

- 12.4.1 Mise en place de journaux d'audit exhaustifs
- 12.4.3 Protection des journaux contre modification ou suppression non autorisée
- 12.4.4 Revue périodique des logs et investigations des anomalies
- 7.2.2 Sensibilisation au rôle des preuves dans la conformité
- 16.1.1 Tests réguliers des dispositifs de traçabilité

R10 : Veille réglementaire insuffisante

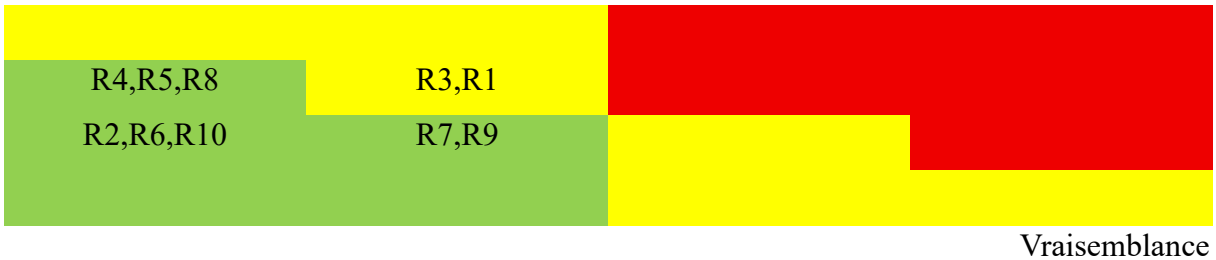
- 18.1.1 Mise en place d'un processus formalisé de veille réglementaire
- 6.1.3 Intégration des évolutions réglementaires dans le SMSI
- 7.1.2 Formation continue sur les évolutions légales et normatives
- 16.1.1 Audit de conformité sur la prise en compte des nouvelles obligations
- 18.2.2 Communication régulière aux parties prenantes des mises à jour

Après application des mesures nous retrouvons la matrice de risque post-traitement

Risque	Gravité avant	Vraisemblance avant	Gravité après	Vraisemblance après	Commentaire synthétique
R1 (Cybercriminels organisés)	Critique	Élevée	Élevée	Moyenne	MFA, détection, patching réduisent vraisemblance, mais gravité reste élevée si intrusion réussie
R2 (Interne malveillant)	Élevée	Moyenne	Moyenne	Faible	Contrôle accès, surveillance et sensibilisation réduisent très fort la vraisemblance et impact
R3 (Prestataire compromis)	Critique	Moyenne/Élevée	Élevée	Moyenne	Contrats, audits et contrôle d'accès diminuent vraisemblance, mais risque impact élevé persiste
R4 (Phishing)	Critique	Élevée	Élevée	Faible	Sensibilisation et MFA réduisent nettement vraisemblance, impact reste élevé si réussite
R5 (Cloud mal configuré)	Critique	Moyenne	Élevée	Faible	Gestion configuration, audits réduisent

					vraisemblance, gravité reste élevée si faille
R6 (Gouvernance insuffisante)	Critique	Moyenne	Moyenne	Faible	Engagement management, pilotage SMSI réduisent vraisemblance, moins impact global
R7 (Doc & contrôles incomplets)	Élevée	Élevée	Moyenne	Moyenne	Meilleure gestion documentaire diminue vraisemblance et gravité (erreurs)
R8 (Prestataire non conforme)	Critique	Moyenne	Élevée	Faible	Audit & formation prestataires réduisent vraisemblance, impact sévère reste possible
R9 (Absence de preuves)	Élevée	Élevée	Moyenne	Moyenne	Mise en place de logs et audits réduit vraisemblance d'erreur et gravité
R10 (Veille réglementaire insuffisante)	Élevée	Moyenne	Moyenne	Faible	Processus veille et formation abaissent risques d'erreurs et impact

Gravité



Vraisemblance

ANNEXE A4 – PLAN DE TRAITEMENT DES RISQUES (PTR)

1. Objectif du plan de traitement

Ce plan vise à définir, pour chaque risque identifié lors de l'analyse EBIOS RM, les mesures de traitement, les responsables, les échéances et le mode de suivi, conformément à ISO/IEC 27001 (6.1.3).

2. Hypothèses de planification

- Démarrage du SMSI : 1er mars 2026
- Horizon de traitement : 12 mois
- Revue trimestrielle par le RSSI
- Arbitrage par la Direction si nécessaire

3. Tableau de traitement des risques

Légende

- Décision : Réduire (R), Éviter (E), Transférer (T), Accepter (A)
- Statut : À lancer / En cours / Terminé

Risques liés au vol de données

ID	Risque	Décision	Mesures principales	Responsable	Échéance	Statut
R1	Phishing entraînant compromission de comptes	R	MFA, sensibilisation, filtrage courriel, SIEM	RSSI	30/06/2026	À lancer

R2	Compromission d'un compte administrateur	R	PAM, revue des droits, journalisation renforcée	DSI	31/07/2026	À lancer
R3	Fuite de données via prestataire	R	Clauses SSI, audits fournisseurs, accès restreints	Achats / RSSI	30/09/2026	À lancer
R4	Exfiltration de données via vulnérabilité applicative	R	Scan de vulnérabilités, patching, WAF	DSI	31/08/2026	À lancer
R5	Vol de sauvegardes	R	Chiffrement, contrôle d'accès, stockage sécurisé	DSI	31/05/2026	À lancer

Risques liés à la non-conformité réglementaire

ID	Risque	Décision	Mesures principales	Responsable	Échéance	Statut
R6	Absence de gouvernance SSI formalisée	R	Nomination RSSI, comités SSI, PSSI	Direction	31/03/2026	À lancer
R7	Non-conformité ISO 27001 / SOC 2	R	SMSI, SoA, audits internes	RSSI	31/12/2026	À lancer
R8	Non-conformité DORA / NIS2	R	Veille réglementaire, gestion incidents, reporting	RSSI / Juridique	30/11/2026	À lancer

R9	Traçabilité insuffisante des actions de sécurité	R	Journalisation, indicateurs SSI, tableaux de bord	RSSI	31/10/2026	À lancer
R10	Absence de preuves lors d'un audit	R	Documentation, archivage, revues périodiques	RSSI	31/12/2026	À lancer

4. Suivi et pilotage du PTR

- Revue trimestrielle de l'avancement par le RSSI
- Mise à jour du registre des risques après chaque revue
- Reporting à la Direction sur les risques critiques
- Réévaluation des risques résiduels après mise en œuvre

5. Validation

- Le présent Plan de Traitement des Risques est validé par la Direction
- Il constitue une entrée majeure du SMSI
- Il est révisé annuellement ou lors de tout changement majeur

GLOSSAIRE DES SIGLES ET ACRONYMES

Sigle	Signification
AC	Autorité de Certification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CNIL	Commission Nationale de l'Informatique et des Libertés
CSP	Cloud Service Provider
DORA	Digital Operational Resilience Act
DSI	Direction des Systèmes d'Information
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité – Risk Manager
IAM	Identity and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISMS	Information Security Management System
MFA	Multi-Factor Authentication
NIS2	Network and Information Security Directive 2
PAM	Privileged Access Management
PCA	Plan de Continuité d'Activité

Sigle	Signification
PRA	Plan de Reprise d'Activité
PSSI	Politique de Sécurité des Systèmes d'Information
PTR	Plan de Traitement des Risques
RACI	Responsible, Accountable, Consulted, Informed
RGPD	Règlement Général sur la Protection des Données
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Système d'Information
SIEM	Security Information and Event Management
SMSI	Système de Management de la Sécurité de l'Information
SOC	Security Operations Center
SoA	Statement of Applicability
SSI	Sécurité des Systèmes d'Information
WAF	Web Application Firewall