Politique de Sécurité des Systèmes d'Information

(PSSI)

WebProd

Version 1.0 | Octobre 2025

Rédigé par : Marc DEVLOP, Gérant et RSSI

Table des matières

Résumé exécutif

Ce document formalise la Politique de Sécurité des Systèmes d'Information (PSSI) de la société WebProd. Il définit le périmètre, les rôles, les principes de sécurité, les mesures de prévention et de mitigation, ainsi que les règles de gestion des incidents et de conformité. La PSSI a pour objectifs principaux : garantir la disponibilité, l'intégrité et la confidentialité des services et données gérés par WebProd.

1 Contexte et périmètre

1.1 Présentation de WebProd

WebProd est une PME spécialisée dans la réalisation et l'hébergement de sites Web pour PME/TPE. Équipe : 4 personnes. Services : développement, hébergement, maintenance.

1.2 Périmètre de la PSSI

La PSSI s'applique à :

- Serveur Active Directory Windows 2019.
- Serveur FTP sous Debian Buster.
- Serveur Web de développement (environnement de préproduction).
- NAS QNAP TS-332X-2G pour sauvegardes locales.
- Postes utilisateur (Windows 10, Debian).
- Commutateur réseau Cisco et passerelle Orange Pro.
- Données clients, documents administratifs, codes sources.

2 Gouvernance et responsabilités

2.1 Rôles et responsabilités

Fonction	Responsabilités SSI
Gérant / RSSI : Marc DEVLOP	Supervision globale, validation de la PSSI, décisionnel en cas d'incident majeur.
Ingénieur système : Ramirez OH	Administration des serveurs, mises à jour, gestion des sauvegardes et de la sécurité technique.
Infographiste : Davi MAGE	Gestion des contenus, respect des consignes de sécurité applicables aux environnements clients.
Secrétaire : Marie GOL	Gestion des données clients et administratives, respect RGPD.
Cabinet comptable (sous-traitant)	Traitement des données comptables sous clause contractuelle et RGPD.

2.2 Principe de responsabilité

Chaque collaborateur applique la PSSI et signale immédiatement au RSSI tout incident ou anomalie.

3 Enjeux et objectifs

— **Disponibilité** : maintenir l'accès aux services et sites clients.
— **Intégrité** : garantir l'exactitude et l'absence d'altération des contenus.
— **Confidentialité** : protéger les données clients et administratives.
— **Continuité** : assurer la reprise d'activité après incident.
— **Conformité** : respecter RGPD et obligations contractuelles.

4 Inventaire des actifs et classification

4.1 Principaux actifs

— Codes sources et repositories clients.
— Environnements de développement et production.
— Données clients et factures.
— Infrastructure réseau et stockage (NAS).
— Comptes d'administration et accès à distance.

4.2 Classification simplifiée

Actif	Niveau de criticité
Codes sources et sites clients	Critique
Serveurs (production / FTP)	Critique
NAS (sauvegardes)	Critique
Données administratives	Important
Postes utilisateurs	Moyen

5 Analyse des risques — Synthèse

5.1 Principaux scénarios de risque

Risque	Impact principal	Mesure prioritaire
Défacement / compromission site client	Perte d'image, perte financière	Durcissement web, correctifs, surveillance, sauvegarde régulière
Intrusion via FTP / fuite de code	Exposition de la propriété intellectuelle	Authentification forte, logs, restriction d'accès
Infection poste utilisateur	Propagation, perte d'activité	Antivirus, politiques d'usage, sauvegarde
Panne NAS / perte sauvegarde	Perte de données critiques	Réplication hors site, test de restauration
Non-conformité RGPD	Sanctions légales	Gestion des droits, durée de conservation, contrats

5.2 Approche d'évaluation

Les risques sont évalués selon une matrice Probabilité x Impact. Les mesures sont priorisées sur la base du rapport coût / réduction de risque.

6 Mesures de sécurité retenues

6.1 Mesures organisationnelles

— Nomination officielle du RSSI.
— Politique de mots de passe : minimum 10 caractères, renouvellement 90 jours, interdiction de comptes partagés.
— Charte d'utilisation des ressources signée par chaque collaborateur.
— Clause de sécurité et confidentialité dans les contrats de sous-traitance.

6.2 Mesures techniques

— Mises à jour régulières et gestion centralisée des correctifs.
— Durcissement des serveurs Debian et Windows (principes de moindre privilège).
— Activation et mise à jour d'antivirus (Kaspersky) sur postes Windows.
— Segmentation réseau : isolation des environnements de développement et production.
— Accès distant sécurisé uniquement via VPN avec authentification forte.
— Journalisation systématique des accès FTP, SSH, RDP et conservation des logs.

6.3 Sauvegardes et continuité

— Sauvegarde quotidienne automatique sur NAS QNAP.

— Réplication mensuelle chiffrée hors site (cloud ou support externe sécurisé).
— Tests de restauration documentés trimestriels.
— Plan de continuité d'activité simplifié précisant les étapes de reprise.

7 Gestion des incidents

7.1 Processus de traitement

1. **Détection** : signalement par utilisateur, alerte système, ou tiers.
2. **Notification** : information immédiate du RSSI.
3. **Confinement** : isolement de l'élément impacté pour limiter la propagation.
4. **Analyse** : identification de la cause racine et évaluation de l'impact.
5. **Remédiation** : application des correctifs, restauration, durcissement.
6. **Communication** : information des clients impactés si nécessaire et tenue d'un registre d'incidents.
7. **Retour d'expérience** : mise à jour des mesures et procédures.

7.2 Registre des incidents

Tout incident significatif est consigné, horodaté et conservé 3 ans. Le registre contient : description, impact, mesures prises, responsables, leçons apprises.

7.3 Escalade et assistance externe

En cas d'incident de sécurité dépassant les compétences techniques ou organisationnelles internes, la société **WebProd** fait appel à un **prestataire externe de cybersécurité ou d'infogérance** habilité.

Procédure d'escalade

1. **Détection** : tout collaborateur signale immédiatement au gérant (RSSI) tout incident suspect, anomalie système ou comportement inhabituel.
2. **Premières mesures internes** :
   — Isolement du poste ou du serveur concerné pour limiter la propagation.
   — Changement immédiat des mots de passe d'administration concernés.
   — Sauvegarde des journaux et éléments de preuve disponibles.
3. **Escalade externe** :
   — Le RSSI (**Marc DEVLOP**) contacte sans délai le **prestataire SSI référent**.
   — Les coordonnées du prestataire (nom, téléphone, courriel, contrat de support) sont tenues à jour dans un **annuaire de crise** annexé à la PSSI.
4. **Assistance technique** :
   — Le prestataire procède à l'analyse, au confinement, à la correction et à la restauration des services impactés.
   — Un **rapport d'incident** est remis à la direction dans les 48 heures suivant la résolution.

5. **Retour d'expérience** :
   — Le RSSI met à jour le registre d'incidents et conserve le rapport dans les archives SSI.
   — La PSSI est ajustée si des failles organisationnelles ou techniques sont identifiées.

Prestataires habilités

— Un **prestataire SSI / infogérant** peut être sollicité pour :
  — assistance technique en cas de compromission,
  — audit ou diagnostic post-incident,
  — restauration des systèmes critiques,
  — conseil pour le renforcement des mesures de sécurité.
— L'hébergeur externe peut également être contacté pour les incidents liés à la mise en production ou à la disponibilité des sites clients.

Principes contractuels

Tout prestataire intervenant sur un incident :
— signe une **clause de confidentialité** couvrant les données internes et celles des clients de WebProd ;
— agit uniquement sous la direction du RSSI ;
— remet un **rapport technique détaillé** mentionnant les causes, actions correctives et recommandations.

8 Sensibilisation et formation

— Sensibilisation annuelle obligatoire sur phishing, mots de passe, bonnes pratiques.
— Formation spécifique des administrateurs sur durcissement et gestion des sauvegardes.
— Exercices de simulation d'incident au moins une fois par an.

9 Conformité et audit

— Conformité RGPD : tenue des registres, droits des personnes, durée de conservation.
— Audit interne semestriel : vérification des sauvegardes, correctifs, gestion des accès.
— Révision annuelle de la PSSI ou après incident majeur.

10 Amélioration continue et SMSI

La PSSI s'inscrit dans une démarche PDCA :
— **Plan** : définir objectifs et mesures.
— **Do** : implémenter la PSSI.
— **Check** : contrôler l'efficacité (audits, KPIs).
— **Act** : corriger et améliorer.

Si la société évolue, un SMSI basé ISO 27001 pourra être déployé de façon progressive.

11 Plan d'action prioritaire (90 jours)

Action	Responsable / Délai
Nomination formelle du RSSI et diffusion PSSI	Marc DEVLOP / 1 semaine
Mise à jour urgente des serveurs et CMS critiques	Ramirez OH / 2 semaines
Activation sauvegardes quotidiennes et test de restauration	Ramirez OH / 2 semaines
Mise en place VPN et restriction accès FTP	Ramirez OH / 3 semaines
Signature de la charte informatique par l'équipe	Marc DEVLOP / 4 semaines
Formation sensibilisation (phishing)	Marc DEVLOP / 6 semaines
Rédaction du registre d'incidents	Ramirez OH / 8 semaines
Vérification contrat cabinet comptable (clause RGPD)	Marc DEVLOP / 10 semaines

Validation et engagement de la direction

Je soussigné, Marc DEVLOP, gérant de WebProd, atteste de l'adoption de la présente PSSI et m'engage à en assurer la mise en oeuvre et le suivi.

Marc DEVLOP, Gérant et RSSI

Historique des versions

Version	Date	Commentaires
1.0	Octobre 2025	Version initiale adaptée à WebProd