CONFIDENTIEL - Usage Interne

POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION

Infrastructure Andrea Hardy

Version 2.0

Février 2026

Auteur: RSSI - Andrea Hardy

Statut: En vigueur

RSSI

Table des matières

1. Gouvernance et Engagement

1.1 Objectifs de la PSSI

Cette Politique de Sécurité du Système d'Information (PSSI) définit le cadre de sécurité pour l'ensemble de l'infrastructure Andrea Hardy. Elle s'applique à tous les actifs informatiques, systèmes, réseaux et données, qu'ils soient hébergés sur site ou dans le cloud.

Cette politique s'impose à toutes les personnes ayant accès au système d'information, qu'elles soient employées, prestataires, ou partenaires.

1.2 Triptyque DIC (Disponibilité, Intégrité, Confidentialité)

Disponibilité

- Les services critiques (WordPress, GLPI, bases de données) doivent être accessibles 99.5% du temps pendant les heures ouvrées.
- Un mécanisme de haute disponibilité avec basculement automatique est mis en place pour les services essentiels.
- Des tests de charge sont effectués trimestriellement pour garantir la performance.

Intégrité

- Les bases de données ne doivent subir aucune modification non autorisée.
- Toute modification est tracée avec horodatage et identification de l'auteur.
- Des contrôles d'intégrité (checksums, signatures) sont appliqués sur les données critiques.
- Les sauvegardes sont protégées contre toute altération par des mécanismes d'immuabilité.

Confidentialité

- Les accès administratifs sont strictement restreints et nécessitent une authentification forte.
- Les données sensibles sont chiffrées au repos et en transit.
- Le principe du moindre privilège est appliqué systématiquement.
- Les accès sont révoqués immédiatement en cas de départ ou de changement de fonction.

1.3 Hébergement et Confidentialité du Document

Cette PSSI est hébergée dans un conteneur isolé, accessible uniquement via le bastion Teleport, afin de garantir que les plans de défense et l'architecture de sécurité restent confidentiels.

2. Organisation et Rôles

2.1 Responsable de la Sécurité des Systèmes d'Information (RSSI)

Responsabilités

- Définir, maintenir et faire évoluer la PSSI
- Superviser les audits de sécurité et tests d'intrusion
- Gérer les incidents de sécurité majeurs
- Valider les changements architecturaux ayant un impact sécurité
- Former et sensibiliser les équipes aux bonnes pratiques
- Assurer la conformité réglementaire (RGPD, etc.)

Droits d'accès

- Accès complet en lecture à tous les systèmes
- Accès d'urgence aux zones critiques (Zone d'Or)
- Consultation de tous les logs et événements de sécurité

2.2 Administrateurs Systèmes

Responsabilités

- Appliquer les configurations de sécurité définies par le RSSI
- Maintenir les systèmes à jour (patches de sécurité)
- Gérer les accès utilisateurs selon le principe du moindre privilège
- Superviser les ressources et détecter les anomalies
- Exécuter les sauvegardes et tests de restauration
- Remonter immédiatement tout incident au RSSI

Droits d'accès

- Accès SSH via bastion Teleport uniquement
- Comptes nominatifs avec traçabilité complète
- Privilèges sudo limités aux tâches nécessaires
- MFA obligatoire pour tous les accès

2.3 Utilisateurs Standards

Responsabilités

- Utiliser les ressources informatiques conformément à la PSSI
- Protéger leurs identifiants et ne jamais les partager
- Signaler immédiatement toute activité suspecte
- Suivre les formations de sensibilisation à la sécurité

Droits d'accès

- Accès limité aux services applicatifs nécessaires (WordPress, GLPI)

- Aucun accès direct aux serveurs ou infrastructures
- Authentification forte avec MFA recommandée

3. Classification des Actifs et Inventaire

3.1 Niveaux de Classification

L'infrastructure est organisée en trois niveaux de criticité :

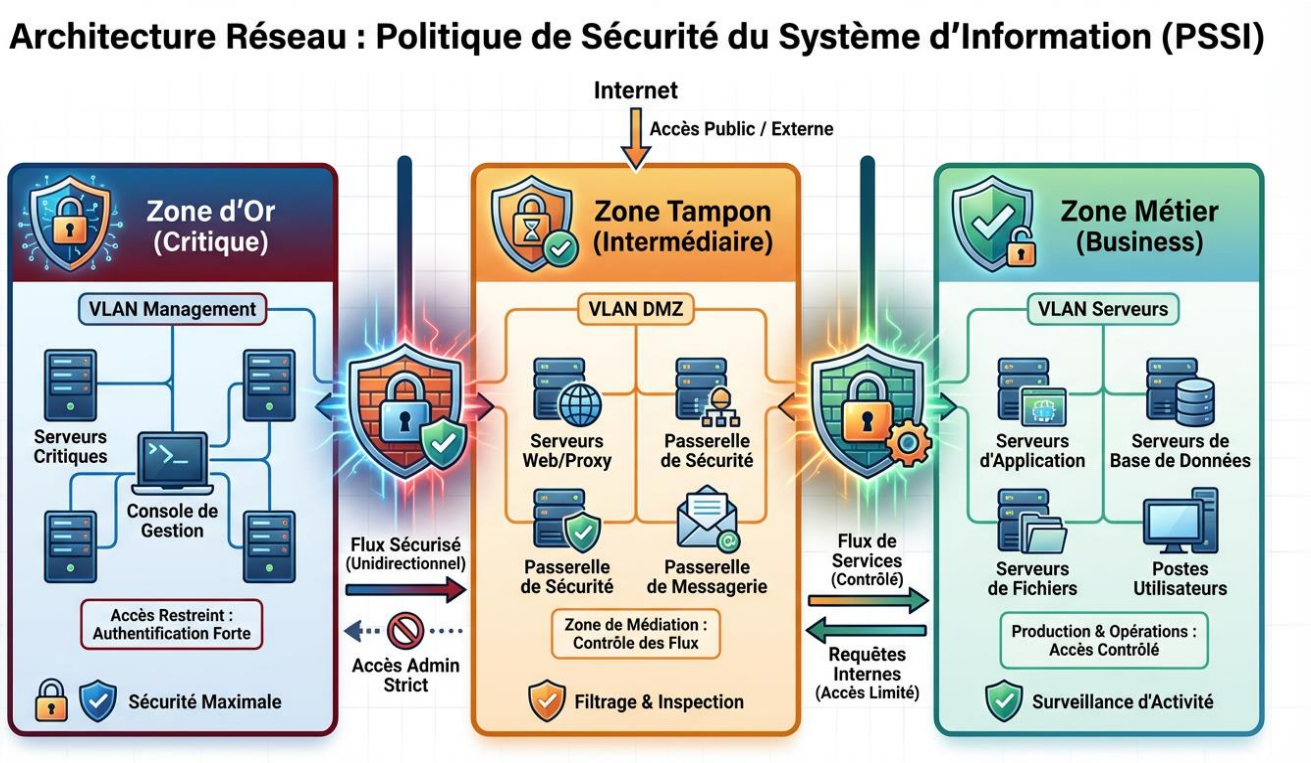
Niveau	Zone	Description
Critique (3)	Zone d'Or - Management	Hyperviseur, équipements réseau, serveurs d'automatisation (Terraform/Ansible)
Interne (2)	Zone Métier - Serveurs	Serveurs applicatifs, bases de données, outils de supervision
Exposée (1)	Zone Tampon - DMZ	Services publics : reverse proxy, partages externes

3.2 Gestion de l'Inventaire

- L'inventaire complet des actifs est maintenu et mis à jour dans GLPI (système de gestion IT).
- Chaque actif est étiqueté avec son niveau de criticité et son propriétaire.
- Une revue trimestrielle de l'inventaire est effectuée pour identifier les actifs obsolètes.
- Tout nouvel équipement doit être enregistré dans GLPI avant sa mise en production.

4. Architecture Réseau et Segmentation

L'infrastructure réseau est segmentée en VLANs isolés, contrôlés par un routeur/pare-feu central. Cette architecture permet de limiter la propagation latérale en cas de compromission.



4.1 Zone d'Or - VLAN Management

C'est la zone la plus sensible de l'infrastructure. Elle héberge les équipements critiques :

- Hyperviseur Proxmox
- Switch de cœur
- Routeur/Pare-feu principal

Règles de sécurité

- Aucun accès vers Internet n'est autorisé depuis cette zone
- L'accès à l'interface de gestion de l'hyperviseur est strictement limité au VLAN Management
- Tout accès nécessite une authentification MFA via le bastion
- Les sessions d'administration sont enregistrées intégralement

4.2 Zone Tampon - VLAN DMZ

Cette zone héberge les services exposés vers l'extérieur ou vers des tiers :

- Reverse proxy (HAProxy) pour WordPress
- Serveur de fichiers Samba pour partages externes
- Contrôleur réseau sans fil (Omada)

Règles de sécurité

- Aucun accès direct vers le VLAN Management
- Les flux vers le VLAN Serveurs sont limités aux requêtes applicatives strictement nécessaires
- Pare-feu applicatif (WAF) activé sur tous les services web
- Limitation de débit (rate limiting) pour prévenir les attaques DDoS

4.3 Zone Métier - VLAN Serveurs

Cette zone contient les serveurs applicatifs et les données métier :

- Serveurs de bases de données (MySQL, PostgreSQL)
- Serveur de supervision (Zabbix)
- Serveur d'orchestration (Terraform/Ansible)
- Serveurs web backend (WordPress, GLPI)

Règles de sécurité

- Les bases de données ne sont jamais exposées directement
- Un reverse proxy dédié (HAProxy DB) filtre tous les accès aux bases
- Les serveurs ne peuvent pas initier de connexions sortantes vers Internet (sauf proxy)
- Chiffrement TLS obligatoire pour toutes les communications inter-serveurs

5. Gestion des Identités et des Accès (IAM)

5.1 Accès Centralisé via Bastion Teleport

Tout accès SSH, RDP ou console vers l'infrastructure doit obligatoirement transiter par le Bastion Teleport. Les connexions directes sont interdites et bloquées par le pare-feu.

Avantages de cette architecture :

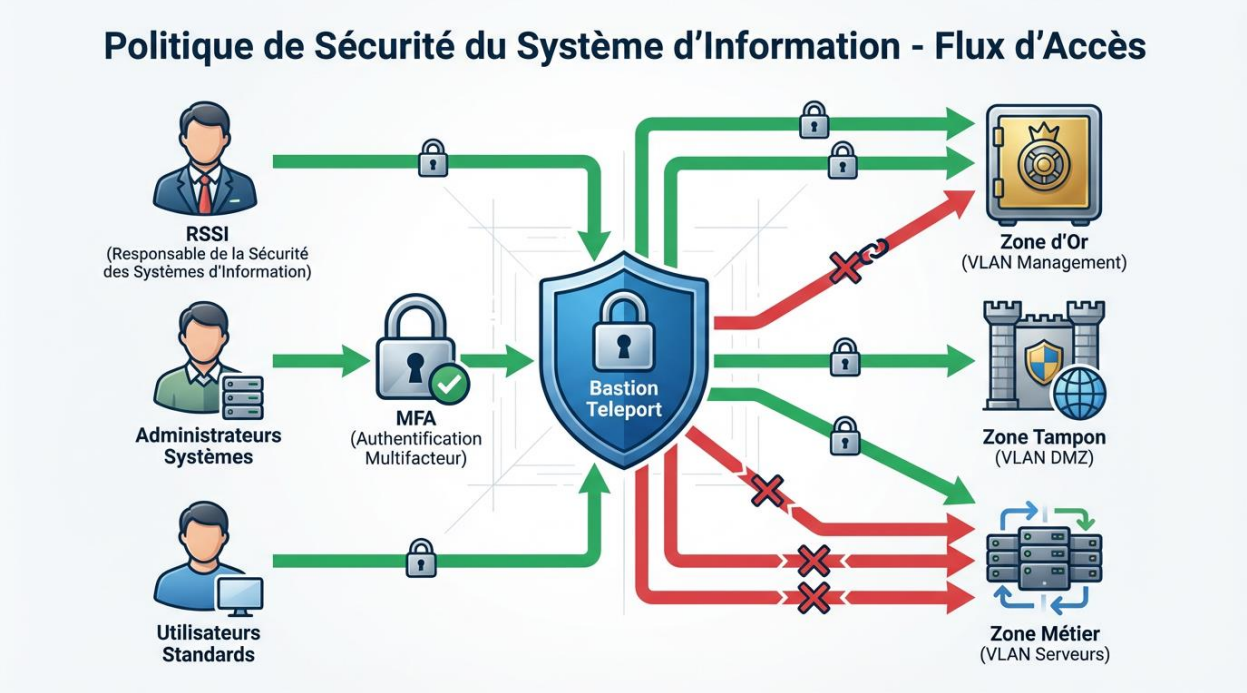
- Point d'entrée unique et contrôlé
- Enregistrement intégral des sessions (video replay)
- Certificats SSH à courte durée de vie (4 heures maximum)
- Révocation instantanée des accès en cas d'incident

5.2 Authentification Multi-Facteurs (MFA)

L'authentification multi-facteurs est obligatoire pour tous les accès privilégiés :

- Accès au bastion Teleport
- Connexion à l'interface d'administration de l'hyperviseur
- Accès aux consoles des routeurs/switches
- Connexion aux serveurs de bases de données

Méthodes MFA acceptées : Application TOTP (Google Authenticator, Authy), clés de sécurité matérielles (YubiKey, FIDO2).



5.3 Gestion des Secrets et Mots de Passe

Tous les mots de passe, clés API et certificats doivent être stockés dans un coffre-fort sécurisé.

Règles applicables :

- Usage de KeePassXC obligatoire pour le stockage local des secrets
- Base de données KeePass protégée par une phrase de passe de 25 caractères minimum
- Rotation des mots de passe tous les 90 jours pour les comptes à privilèges
- Interdiction formelle de stocker des mots de passe en clair (fichiers texte, post-it, etc.)
- Les clés SSH sont générées avec au minimum 4096 bits (RSA) ou ED25519

6. Sécurité des Hyperviseurs et Infrastructure as Code

6.1 Sécurité de l'Hyperviseur Proxmox

L'hyperviseur est le socle de confiance de toute l'infrastructure. Sa compromission aurait des conséquences catastrophiques.

Mesures de protection :

- Accès HTTPS uniquement avec certificat valide
- Désactivation de l'authentification par mot de passe (clés SSH uniquement)
- Comptes nominatifs obligatoires (pas de compte partagé)
- Journalisation de toutes les actions d'administration
- Mise à jour mensuelle des correctifs de sécurité
- Surveillance en temps réel des processus et de la charge CPU

6.2 Infrastructure as Code (Terraform / Ansible)

Le serveur d'orchestration est le "cerveau" de la configuration automatisée. Il possède des privilèges étendus et doit être particulièrement protégé.

Mesures de sécurité :

- Accès restreint au RSSI et aux administrateurs seniors uniquement
- Fail2ban activé pour bloquer les tentatives de bruteforce
- Tous les scripts Terraform/Ansible sont versionnés dans un dépôt Git privé
- Validation obligatoire (code review) avant toute modification
- Tests en environnement de pré-production avant déploiement
- Logs d'audit conservés pendant 1 an minimum

7. Sécurité des Services et Durcissement

7.1 Serveurs Web et Applicatifs

Chaque machine virtuelle ou conteneur subit un processus de durcissement (hardening) avant sa mise en production.

Standards de durcissement :

- Désinstallation de tous les services inutiles
- Configuration des mises à jour automatiques pour les correctifs critiques
- Pare-feu local (iptables/nftables) autorisant uniquement les flux nécessaires
- Désactivation des comptes système par défaut
- Bannières de connexion informant du caractère surveillé des accès
- SELinux ou AppArmor activé en mode enforcing

7.2 Validation des Configurations

Avant la mise en production, chaque serveur est audité avec des outils automatisés :

- Lynis pour l'audit de sécurité système
- OpenSCAP pour la conformité aux benchmarks CIS
- Nmap pour identifier les ports ouverts
- Checklists de validation signées par le RSSI

8. Supervision, Journalisation et Traçabilité

8.1 Supervision des Ressources (Zabbix)

Le serveur Zabbix surveille en temps réel la disponibilité et les performances de tous les équipements et services.

Métriques surveillées :

- Disponibilité des services (HTTP, MySQL, SSH)
- Charge CPU et mémoire
- Espace disque disponible
- Trafic réseau et bande passante
- Température et état des équipements physiques

Alertes et escalades :

- **Critique :** Notification immédiate au RSSI et aux administrateurs (SMS + Email)
- **Haute :** Email aux administrateurs avec délai de 15 minutes
- **Moyenne :** Tableau de bord uniquement

Toute chute de performance CPU inexpliquée est traitée comme un incident de sécurité potentiel (cryptomining, ransomware, botnet).

8.2 Journalisation Centralisée

Tous les événements de sécurité et d'administration sont enregistrés de manière centralisée.

Sources de logs :

- **Pare-feu :** Connexions bloquées, tentatives d'intrusion
- **Bastion Teleport :** Sessions SSH, commandes exécutées
- **Serveurs :** Authentifications, erreurs système, accès aux fichiers sensibles
- **Applications :** Erreurs, tentatives d'accès non autorisées

Durée de conservation :

- Logs de sécurité : 12 mois minimum
- Logs d'audit (accès privilégiés) : 24 mois
- Logs applicatifs : 3 mois

8.3 Traçabilité des Actions Administratives

La traçabilité complète des actions à privilèges est essentielle pour la sécurité et la conformité.

Informations enregistrées :

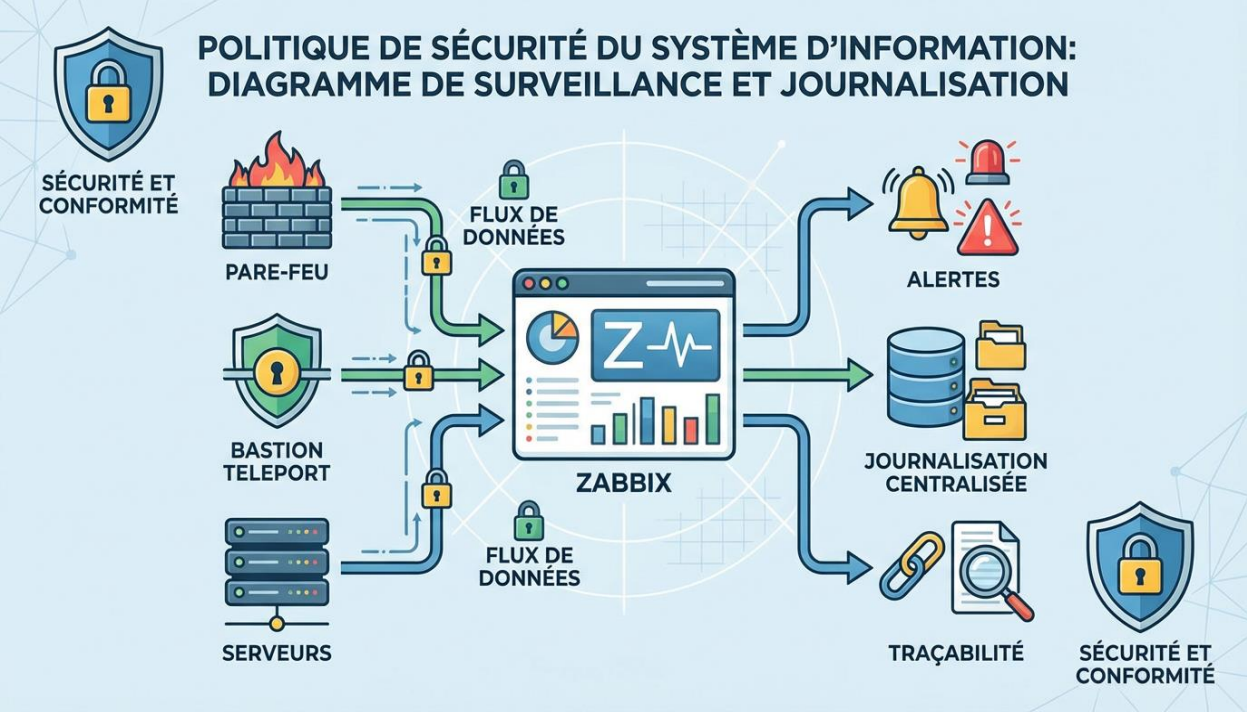
- Identité de l'administrateur (compte nominatif)

- Date et heure précise de la connexion
- Serveur ou équipement accédé
- Toutes les commandes exécutées
- Modifications de configuration effectuées
- Durée de la session

Le bastion Teleport enregistre également les sessions en vidéo (terminal replay), permettant de rejouer exactement ce qui s'est passé en cas d'incident.

Contrôles d'accès aux logs :

- Seul le RSSI a accès complet aux logs
- Les administrateurs peuvent consulter leurs propres logs
- Toute consultation de logs est elle-même tracée
- Les logs sont protégés en intégrité (signature, WORM)



9. Gestion des Incidents de Sécurité

9.1 Détection et Alerte

Les incidents de sécurité peuvent être détectés par plusieurs moyens :

- Alertes Zabbix (anomalies de performance, services down)
- Logs du pare-feu (tentatives d'intrusion, scans de ports)
- Fail2ban (tentatives de bruteforce)
- Signalements des utilisateurs
- Audits de sécurité réguliers

9.2 Procédure de Réponse à Incident

En cas de détection d'un incident de sécurité, la procédure suivante est appliquée :

- **1. Alerte :** Notification immédiate du RSSI et de l'équipe d'astreinte
- **2. Évaluation :** Analyse rapide de la gravité et de l'impact
- **3. Confinement :** Isolation immédiate du système compromis via le pare-feu
- **4. Éradication :** Suppression de la menace (malware, compte compromis, vulnérabilité)
- **5. Récupération :** Restauration du service depuis une sauvegarde saine
- **6. Analyse post-incident :** Rapport détaillé et leçons apprises

9.3 Post-Incident et Amélioration Continue

Après chaque incident de sécurité, un rapport d'analyse est rédigé incluant :

- Chronologie détaillée des événements
- Cause racine identifiée
- Impact sur les services et les données
- Actions correctives mises en place
- Recommandations pour éviter la récurrence

Ce rapport est présenté à la direction et conservé dans le registre des incidents.

10. Conformité et Évolutions

10.1 Audits de Sécurité

La conformité de l'infrastructure à cette PSSI est vérifiée régulièrement :

Audits internes :

- Revue trimestrielle des configurations de sécurité
- Vérification mensuelle des droits d'accès
- Analyse des logs de sécurité chaque semaine

Audits externes :

- Test de pénétration interne annuel
- Audit de conformité RGPD si traitement de données personnelles
- Scan de vulnérabilités mensuel avec outils automatisés

10.2 Évolutions Prévues

Cette politique de sécurité est un document vivant qui évolue avec l'infrastructure.

Prochaines améliorations planifiées :

- **Q1 2026 :** Mise en œuvre de l'immuabilité des sauvegardes Veeam (protection contre ransomware)
- **Q2 2026 :** Déploiement d'un SIEM (Security Information and Event Management) pour corrélation des logs
- **Q3 2026 :** Mise en place d'une architecture Zero Trust avec micro-segmentation
- **Q4 2026 :** Chiffrement de bout en bout de toutes les communications inter-serveurs

Cette PSSI est revue annuellement et mise à jour en fonction des évolutions technologiques, réglementaires et des menaces.

_____

RSSI Andrea Hardy
Février 2026