POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (PSSI) - XANADU

Version : 1.0

Date de validation : A définir

Validé par : Direction Générale XANADU

1. Contexte et Objectifs

La présente politique définit les exigences de sécurité pour le système d'information (SI) de XANADU dans le cadre de son installation sur la technopole Atlantis et le déploiement du site de Springfield.

Face à la recrudescence des cybermenaces (notamment les rançongiciels), cette politique vise quatre objectifs fondamentaux :

- **Disponibilité :** Garantir un RTO (Temps de rétablissement) de **4 heures** pour les services critiques et de 24 heures pour les autres.
- **Intégrité :** Protéger les données contre toute altération non autorisée (notamment la base ERP et les fichiers financiers).
- **Confidentialité :** Assurer que les données sensibles (RH, Juridique, Direction) ne sont accessibles qu'aux personnes habilitées.
- **Traçabilité :** Enregistrer et conserver les traces d'accès et d'administration pour permettre l'audit post-incident.

2. Périmètre d'application

Cette politique s'applique à l'ensemble du périmètre XANADU :

Le périmètre géographique de l'infrastructure s'étend sur deux localisations distinctes, constituées du siège social nommé « Atlantis » et du site distant « Springfield ».

Cette architecture dessert une population d'utilisateurs hétérogène comprenant l'ensemble des soixante collaborateurs internes, répartis à raison de cinquante personnes sur le site principal et dix sur le site secondaire, auxquels s'ajoutent les effectifs en télétravail, les prestataires externes ainsi que les stagiaires.

D'un point de vue matériel, le périmètre technique concerne la totalité des actifs connectés au système d'information, englobant les serveurs, les postes de travail, les infrastructures réseaux ainsi que les terminaux mobiles.

3. Classification des Données

Les données gérées par XANADU sont classifiées selon leur niveau de sensibilité et de disponibilité requis:

Niveau	Description / Exemples	Exigences RTO/RPO
C1 - Critique	Données dont la perte bloque l'entreprise. *(Base ERP PostgreSQL, Partages Direction/Juridique)*	**RTO :** 4h **RPO :** 3h
C2 - Important	Données nécessaires au fonctionnement quotidien. *(Documents Commerciaux, Emails, RH)*	**RTO :** 24h **RPO :** 12h
C3 - Standard	Données personnelles ou temporaires. *(Dossiers "Mes Documents" des utilisateurs)*	**RTO :** 24h **RPO :** 24h

4. Sécurité des Accès et Gestion des Identités (IAM)

4.1. Identification et Authentification

La politique d'identification impose l'attribution d'un compte unique et nominatif à chaque utilisateur, suivant le format standardisé « p.nom », tout en proscrivant formellement l'usage de comptes génériques.

L'authentification est sécurisée par des mots de passe robustes de douze caractères minimum respectant des critères de complexité stricts et gérés par stratégie de groupe

(GPO), incluant un mécanisme de verrouillage automatique du compte après trois tentatives infructueuses.

Par ailleurs, le principe du moindre privilège est appliqué rigoureusement sur l'ensemble du parc, interdisant aux utilisateurs de disposer des droits d'administration locale sur leurs postes de travail.

4.2. Administration

En ce qui concerne les opérations de maintenance et de gestion, une séparation stricte des environnements est mise en œuvre.

Les administrateurs systèmes ont l'obligation d'utiliser un compte dédié exclusivement aux tâches d'administration (de type adm_user), totalement distinct de leur compte bureautique habituel.

Enfin, dans le cadre du télétravail ou de la mobilité, l'accès distant aux ressources internes s'effectue uniquement au travers d'un tunnel VPN sécurisé utilisant un chiffrement AES-256 et s'appuyant sur une authentification centralisée.

5. Sécurité du Réseau et des Flux

5.1. Cloisonnement (Segmentation)

Le réseau est segmenté en VLANs étanches par service (RH, Compta, IT, etc.) pour limiter la propagation latérale des attaques. Les flux inter-VLAN sont filtrés par un pare-feu interne.

5.2. Filtrage Périmétrique

- **Principe "Block All" :** Par défaut, tout flux réseau non explicitement autorisé est interdit.
- **Architecture DMZ :** Les services exposés sont isolés dans une DMZ protégée par une double barrière de pare-feu (Architecture "Sandwich" ou “3 pattes”).
- **Accès Internet :** La navigation Web est filtrée par un Proxy (Squid) interdisant l'accès aux sites malveillants ou non conformes à la charte.

6. Sécurisation des Postes et Serveurs (Durcissement)

La protection contre les menaces numériques repose sur le déploiement généralisé et actif d'une solution de défense multicouche, intégrant Antivirus, EDR et XDR, sur la totalité du parc informatique comprenant les serveurs et les postes de travail.

En parallèle, le maintien du niveau de sécurité est assuré par une gestion centralisée des correctifs via WSUS, imposant l'installation automatique des mises à jour critiques du système et des applications sans possibilité d'interruption par l'utilisateur.

Enfin, pour prévenir l'exfiltration d'informations sensibles et l'introduction de codes malveillants, des restrictions techniques bloquent l'utilisation de tout support amovible personnel, incluant les clés USB et les disques externes

7. Continuité d'Activité et Sauvegardes

La stratégie de sauvegarde respecte la règle du **3-2-1** pour garantir la résilience face aux rançongiciels:

- **3 copies** des données.
- **2 supports** différents (Stockage local RAID 10/RAID 6).
- **1 copie hors site** (Réplication automatique entre Atlantis et Springfield via lien MPLS chiffré).
- **Immuabilité :** Les sauvegardes critiques sont protégées contre la modification et la suppression (Inaltérabilité).

Des tests de restauration sont effectués périodiquement pour valider l'intégrité des sauvegardes.

8. Surveillance et Gestion des Incidents

La surveillance de l'activité du système d'information repose sur la centralisation systématique des événements de sécurité vers un serveur de supervision SIEM Wazuh.

Ce dispositif assure la collecte et l'analyse continue des traces relatives aux connexions, aux accès aux fichiers critiques ainsi qu'aux alertes générées par les pare-feux.

En complément de cette surveillance technique, la sécurité opérationnelle implique la vigilance de chacun : tout utilisateur constatant une anomalie, qu'il s'agisse de lenteurs injustifiées, de fichiers suspects ou de tentatives de phishing, a l'obligation d'alerter immédiatement le service informatique.

9. Contrôle et Sanctions

Le respect de la présente PSSI est obligatoire.

Des audits réguliers (tests d'intrusion, revue des droits d'accès) sont menés pour vérifier sa bonne application.

Le non-respect de ces règles expose le contrevenant à des sanctions disciplinaires conformément au règlement intérieur.

Lu et approuvé.

Nom et Prénom : _____

Date : _____ / _____ / _____

Signature :