**🛡️ Politique de Sécurité des Systèmes d'Information (PSSI) – OptiValue**

**1. Préambule**

La sécurité des systèmes d’information (SI) est un enjeu stratégique pour **OptiValue**, dont l’activité repose sur la fiabilité, l’intégrité et la confidentialité des données. Cette politique vise à encadrer l’usage, la protection, et la résilience du SI contre les menaces internes et externes.

**2. Objectifs de la PSSI**

* Garantir la **disponibilité** des systèmes critiques.
* Assurer la **confidentialité** des informations sensibles (clients, partenaires, internes).
* Préserver l’**intégrité** des données.
* Se conformer aux exigences réglementaires (RGPD, ISO 27001, NIS2, etc.).
* Instaurer une culture de **cybersécurité** au sein de l’entreprise.

**3. Champ d’application**

La PSSI s’applique à :

* Tous les collaborateurs, prestataires, stagiaires et partenaires ayant accès au SI.
* Tous les équipements, logiciels, réseaux et données appartenant ou exploités par OptiValue.

**4. Gouvernance de la sécurité**

| **Rôle** | **Responsabilité** |
| --- | --- |
| **RSSI** (Responsable Sécurité SI) | Pilote la stratégie, audite les pratiques, anime la sensibilisation |
| **DSI** | Supervise les opérations IT et la mise en œuvre technique des mesures |
| **Comité SSI** | Valide la politique, les plans d’action, gère les incidents majeurs |
| **Direction Générale** | Porte la politique et garantit les moyens associés |

**5. Gestion des risques**

* Réalisation annuelle d’une **analyse de risques** (EBIOS RM).
* Élaboration de plans de **traitement**, avec priorisation selon la criticité.
* Suivi des actions de réduction de risque (PRA, PCA, patchs…).

**6. Classification de l'information**

| **Niveau** | **Description** | **Exemples** |
| --- | --- | --- |
| **Public** | Données librement diffusables | Communiqués de presse |
| **Interne** | Données à usage professionnel en interne | Procédures RH |
| **Confidentiel** | Données sensibles à protéger | Données clients, contrats |
| **Strictement confidentiel** | Données critiques à diffusion restreinte | Algorithmes, projets R&D |

**7. Sécurité physique et logique**

**7.1 Sécurité physique**

* Contrôle d’accès badge aux locaux.
* Vidéosurveillance des zones sensibles.
* Locaux serveurs isolés et verrouillés.

**7.2 Sécurité logique**

* Authentification forte (MFA) sur tous les systèmes critiques.
* Gestion centralisée des identités (IAM).
* Chiffrement des données sensibles (au repos et en transit).
* Cloisonnement des réseaux (VLAN, DMZ).

**8. Contrôle des accès**

* Principe du **moindre privilège**.
* Gestion des droits via des rôles (RBAC).
* Révocation immédiate des accès en cas de départ.
* Revue régulière des habilitations.

**9. Protection contre les menaces**

* Antivirus / EDR déployés sur tous les terminaux.
* Firewall de nouvelle génération (NGFW) en bordure de réseau.
* Analyse comportementale des connexions (SIEM / SOC).
* Tests de pénétration et audits réguliers.

**10. Gestion des incidents de sécurité**

* Déclaration obligatoire de tout incident par les utilisateurs.
* Procédure de réponse : détection → confinement → éradication → reprise → post-mortem.
* Tenue d’un **registre des incidents**.
* Communication à l’ANSSI et à la CNIL si nécessaire.

**11. Plan de continuité et de reprise**

* **PCA** : maintien des processus critiques (infogérance, backup cloud, redondance).
* **PRA** : restauration sous 4 à 24h en cas de sinistre majeur.
* Tests semestriels des scénarios de crise.

**12. Sensibilisation et formation**

* Formation annuelle à la cybersécurité pour tous les collaborateurs.
* Exercices de phishing simulés.
* Guide des bonnes pratiques numériques distribué dès l’intégration.

**13. Relations avec les tiers**

* Clauses de sécurité dans tous les contrats de sous-traitance.
* Contrôles d’accès limités pour les partenaires.
* Audits réguliers des fournisseurs critiques.

**14. Conformité et audit**

* Alignement avec le **référentiel ISO/IEC 27001**.
* Audit interne annuel.
* Plan de conformité RGPD supervisé par le DPO.

**15. Évolution de la politique**

* Révision de la PSSI au moins une fois par an.
* Mise à jour après tout événement majeur (incident, évolution réglementaire).
* Communication formelle aux utilisateurs à chaque mise à jour.

**16. Annexes (exemples)**

* A1. Politique de mots de passe
* A2. Charte informatique
* A3. Procédure d’habilitation
* A4. Plan de gestion de crise
* A5. Modèle d’analyse de risques