**Annexes détaillées – Politique de Sécurité des Systèmes d’Information d’OptiValue**

**Référence interne :** PSSI‑2025‑ANNEXES v1.0

**Date de validation :** 29 juillet 2025  
**Prochaine révision :** juillet 2026

**A1 – Politique de mots de passe**

**1. Objectif**

Garantir la robustesse et la bonne gestion des secrets d’authentification afin de limiter les risques de compromission d’identité.

**2. Portée**

S’applique à tous les comptes utilisateur, administrateur, comptes de service, clefs API et coffres d’identifiants gérés par OptiValue.

**3. Exigences de création de mot de passe**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type de compte** | **Longueur minimale** | **Complexité requise** | **Expiration** | **Historique** | **MFA obligatoire** |
| Utilisateur standard | 12 car. | 3 classes sur 4\* | 365 jours | 12 anciens | Oui |
| Compte privilégié (admin, root) | 16 car. | 4 classes | 90 jours | 24 anciens | Oui (FIDO2) |
| Compte de service | 24 car. | Aléatoire, généré par coffre | Changement automatique 180 jours | Non applicable | Non (clé API) |

\* Classes : majuscule, minuscule, chiffre, caractère spécial.

**4. Stockage et transmission**

* Tous les secrets sont stockés sous forme **hashée (bcrypt, coût 12)** ou chiffrée dans un coffre de secrets (HashiCorp Vault).
* Aucune diffusion de mot de passe par e‑mail ou messagerie instantanée non chiffrée.
* Les liens de réinitialisation expirent en 30 minutes.

**5. Utilisation et renouvellement**

* Interdiction de réutiliser un mot de passe professionnel à titre privé.
* Les mots de passe doivent rester **personnels et non partagés** ; l’usage d’un coffre partagé chiffré (KeePassXC) est autorisé pour les identifiants applicatifs collectifs.
* Tout changement de mot de passe doit être initié depuis le portail IAM.

**6. Comptes privilégiés**

* Obligation de recourir à un **bastion** pour l’élévation de privilèges.
* Journalisation détaillée des connexions et commandes.

**7. Comptes de service & API**

* Rotation automatique via pipeline CI/CD.
* Droits les plus faibles possibles (principe **PoLP**).

**8. Contrôles et conformité**

* Audit trimestriel des bases de comptes via outils d’**exposition de hachage** (HaveIBeenPwned).
* Tests de robustesse systématiques lors des pentests internes.

**9. Gestion des incidents**

* Compromission suspectée → réinitialisation immédiate + enquête SOC.
* Notification au RSSI et, si données personnelles impactées, au DPO.

**A2 – Charte d’usage des ressources informatiques**

**1. Finalité**

Définir les règles d’utilisation acceptable des équipements, réseaux et applications d’OptiValue.

**2. Principes généraux**

1. **Responsabilité individuelle** : chaque utilisateur est gardien des ressources qu’il utilise.
2. **Usage professionnel prioritaire** : l’utilisation personnelle est tolérée si raisonnable et non contraire à la loi.

**3. Comportements attendus**

* **Poste de travail** : système à jour, verrouillage < 5 min, chiffrement disque (BitLocker/FileVault).
* **Courriel** : signature pro, vigilance hameçonnage, aucune donnée « Confidentiel » non chiffrée.
* **Internet** : accès aux sites licites ; streaming, peer‑to‑peer interdits.
* **Logiciels** : installation uniquement via le catalogue approuvé (Intune Self‑Service).
* **Réseaux sociaux** : mention explicite que les propos n’engagent pas OptiValue, respect du secret des affaires.

**4. Télétravail et mobilité**

* Accès via **VPN IPsec + MFA** obligatoire hors site.
* Utilisation exclusive d’équipements gérés MDM.

**5. Données sensibles**

* Respect de la classification (cf. chapitre 6 de la PSSI).
* Chiffrement AES‑256 pour tout stockage sur support amovible.

**6. Contrôle et sanctions**

* Logs conservés 12 mois (SIEM).
* Non‑respect → rappel → avertissement → procédures RH / disciplinaire.

**A3 – Procédure d’habilitation (gestion des accès)**

**1. Cycle de vie d’une habilitation**

|  |  |  |  |
| --- | --- | --- | --- |
| Étape | Acteur | Délai cible | Preuve |
| Demande d’accès | Manager | J0 | Ticket JIRA « Access Request » |
| Validation | Data Owner + RSSI (si sensible) | < 2 jours | Approbation numérique |
| Mise en œuvre | Équipe IAM | < 1 jour | Journal IAM |
| Contrôle post‑mise | Manager | < 5 jours | Check‑list onboard |
| Revue périodique | Data Owner | trimestriel | Rapport revue |
| Révocation | RH + IAM | J0 départ | Script off‑boarding |

**2. Règles spécifiques**

* **Séparation des tâches** obligatoire : aucun dev n’a accès à prod en direct.
* **Accès temporaires** : durée max 30 jours, suppression auto.
* **Accès d’urgence** : bastion break‑glass, journalisation complète, validité 6 h.

**3. Matrice RACI**

R: Responsable de l’action ; A: Autorité de décision ; C: Consulté ; I: Informé.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Habilitation | Manager | Data Owner | IAM | RSSI |
| Attribution | R | A | C | I |
| Révocation | R | I | A | C |
| Revue périodique | C | A | I | R |

**4. Traçabilité**

Tous les changements sont consignés dans le SIEM (Elastic + Auditbeat) et conservés 5 ans.

**A4 – Plan de gestion de crise (PGC)**

**1. Objectifs**

* Protéger les personnes, les actifs et l’image de l’entreprise.
* Restaurer l’activité à un niveau acceptable (**RTO 24 h**, **RPO 4 h**).

**2. Scénarios de référence**

1. **Cyber‑attaque majeure** (ransomware, fuite de données).
2. **Panne d’infrastructure** (cloud provider outage).
3. **Sinistre physique** (incendie datacenter, inondation siège).
4. **Pandémie / indisponibilité RH massive**.

**3. Organisation de crise**

|  |  |  |  |
| --- | --- | --- | --- |
| Rôle | Titulaire | Suppléant | Missions principales |
| Directeur de crise | COO | CEO | Décision stratégique, arbitrage budget |
| Commandement opérationnel | RSSI | DSI | Coordination technique |
| Communication externe | Dir. Com | Juriste | Relation presse, régulateur |
| Support juridique | Juriste | DPO | Notification CNIL, contrats fournisseurs |
| Log keeper | PMO | — | Journal d’événements |

**4. Processus d’activation**

* **Seuil d’alerte 3** atteint (incident critique) → appel astreinte RSSI.
* Réunion virtuelle « War Room » (< 30 min).
* Émission d’un **CR d’activation** (modèle PGC‑ACT‑01).

**5. Phases**

1. Détection & évaluation (SOC – 15 min).
2. Confinement (isolation réseau, sauvegarde forensique).
3. Rémédiation (patch, restauration, key‑rotation).
4. Reprise d’activité (validation, smoke‑tests).
5. Clôture & **REX** sous 10 jours.

**6. Communication**

* Messages internes via Teams + SMS fallback.
* Communiqués externes validés par juridique et DG.

**7. Exercices**

* 2 crisis‑drills par an (table‑top + jeu de rôle technique).
* Bilan présenté au Comité SSI.

**A5 – Modèle d’analyse de risques**

**1. Méthodologie retenue**

Adaptation d’**EBIOS Risk Manager** version 2022.

**2. Étapes détaillées**

1. **Cadre du risque** : contexte business, périmètre SI, contraintes réglementaires.
2. **Étude des événements redoutés** : altération, divulgation, indisponibilité, usurpation.
3. **Cartographie des biens essentiels** : données, processus, services.
4. **Sources de menace** : internes, externes, opportunistes, étatiques.
5. **Scénarios crédibles** : association biens + menace + mode opératoire.
6. **Évaluation** :
   * **Vraisemblance** : Échelle 1‑5 (historique incidents, exposition, motivation).
   * **Impact** : Échelle 1‑5 (financier, réputation, légal, opérationnel).
7. **Niveau de risque** = Vraisemblance × Impact (matrice 5×5).
8. **Traitement** : réduction, transfert, acceptation, évitement.
9. **Plan d’action** : pilote, budget, échéance, KPI.

**3. Critères d’acceptation**

* Risque évalué ≤ 6 (sur 25) : accepté par le Data Owner.
* Risque 7‑15 : plan d’atténuation < 6 mois.
* Risque > 15 : escalade DG, actions immédiates.

**4. Reporting**

* **Registre de risques** central (Confluence) mis à jour mensuellement.
* Tableau de bord Power BI présenté au Comité SSI.

**5. Maintien à jour**

* Analyse complète annuelle ou lors de changement majeur SI.
* Validation par RSSI et Direction.