Politique de Sécurité du Système d’Information de CovY

- Version : 2.3
- Date : juillet 2025
- Classification : Interne – Ne pas diffuser
- Pilotage : Adel B : Directeur de CovY / Caulin L : Chef de la Sécurité (RSSI)

CovV | https://paraweb.fr/Covy/ | adelB-caulinL@covy-security-ynov.fr

2 Introduction, contexte & périmètre

2.1 Introduction

La présente Politique de Sécurité des Systèmes d'Information (PSSI) a pour objectif de définir les principes et règles à respecter pour sécuriser la plateforme e-commerce CovY et ses environnements associés, dans le cadre d'un fonctionnement 100 % full remote. Elle s'appuie sur les bonnes pratiques de la norme ISO 27001 ainsi que sur les exigences du Règlement Général sur la Protection des Données (RGPD).

2.2 Contexte

• CovY est une entreprise d'e-commerce offrant produits et services en ligne via le site https://paraweb.fr/Covy/ecommerce-pro.html
• En raison de la pandémie et des mesures de distanciation, l'ensemble des collaborateurs (10 personnes) sont désormais en télétravail répartis sur tout le territoire français.
• La plateforme traite des données clients à caractère personnel (identité, coordonnées, informations de paiement…), soumises aux obligations du RGPD.
• L'entreprise souhaite garantir la confidentialité, l'intégrité et la disponibilité de son service, tout en assurant la continuité d'activité et la conformité ISO 27001.

2.3 Périmètre

2.3.1 Actifs et services couverts

– Site web e-commerce (page de vente, panier, paiement)
– Back-office administrateur (gestion des commandes, produits, promotions)
– API internes et tierces (CRM, ERP, service d'emailing, passerelles de paiement)
– Infrastructure réseau (VPN, pare-feux, zones cloud, dmz)
– Postes de travail des salariés (systèmes d'exploitation, applications métiers, VPN client)

2.3.2 Utilisateurs et localisations

– Dix collaborateurs en full remote, situés dans différentes régions de France.
– Accès autorisés depuis postes fixes (domiciles) préalablement enregistrés.

2.3.3 Exclusions

– Les services externalisés non relatifs à la plateforme de production (ex : hébergement de messagerie grand public) ne sont pas couverts, sauf si leur utilisation implique le traitement de données clients.

2.4 Objectifs de sécurité

– Garantir la confidentialité et la protection des données personnelles des clients (conformité RGPD).

– Assurer la disponibilité du service e-commerce (objectif de 99,9 % uptime).
– Prévenir, détecter et répondre aux incidents de sécurité (ISO 27001).
– Mettre en place un dispositif de contrôle d’accès, d’authentification forte et de chiffrement adapté au télétravail.

2.5 Acteurs et rôles
– Adel B : Directeur de CovY – Responsable de la validation de la PSSI et des arbitrages budgétaires.
– Caulin L : Co-créateur et Chef de la Sécurité (RSSI) – Pilotage de la mise en œuvre, suivi des risques et reporting.
– Collaborateurs à distance – Respect des procédures d’accès, signalement des incidents et participation aux formations.

3 Gouvernance de la sécurité & référentiels

3.1 Politique de sécurité

• Objectif général
– Protéger la confidentialité, l'intégrité et la disponibilité de l'information liée à la plateforme CovY.
– Assurer la conformité aux exigences légales (RGPD) et normatives (ISO 27001).
• Principes directeurs
– Application du principe du moindre privilège
– Gestion proactive des risques et incidents
– Responsabilisation de chaque collaborateur
– Amélioration continue via la roue PDCA (Plan–Do–Check–Act)

3.2 Organisation de la gouvernance

• Comité de pilotage sécurité
– Composition : Adel B (Direction), Caulin L (RSSI), DPO (interne ou prestataire externe) , Responsable IT, représentant RH
– Rôle : arbitrer les budgets sécurité, valider la PSSI, suivre les plans d'action
– Fréquence des réunions : à minima semestrielle
• Revue de Direction
– Fréquence : annuelle (ou à chaque changement majeur)
– Sujets : résultat des audits, état des risques, indicateurs sécurité, conformité RGPD
• Missions du RSSI (Caulin L)
– Animation du processus de gestion des risques et des incidents
– Pilotage de la mise en œuvre des mesures de sécurité
– Reporting au Comité de pilotage
• Délégué à la Protection des Données (DPO)
– Garantie du respect des droits des personnes (droits d'accès, d'effacement…)
– Réalisation et mise à jour du registre des traitements
– Réalisation des analyses d'impact (DPIA) sur les traitements sensibles

3.3 Référentiels et normes

• ISO 27001:2013
– Application des contrôles de l'Annexe A adaptés au contexte full remote
– Mise en place d'un Système de Management de la Sécurité de l'Information (SMSI)
• RGPD
– Principes : licéité, loyauté, transparence, limitation des finalités, minimisation, exactitude, conservation limitée, sécurité
– Processus : registre des traitements, information des personnes, procédures de gestion des violations de données
• Autres bonnes pratiques citées
– ISO 27005 / EBIOS pour l'analyse de risques

– Recommandations ANSSI pour la sécurisation du télétravail
– Guides PCI-DSS pour la gestion des paiements en ligne

3.4 Audits internes et externes
• Audit interne
– Fréquence : annuel, conduit par le RSSI et/ou un auditeur interne identifié
– Portée : conformité ISO 27001 (SMSI), RGPD, respect des procédures full remote
• Audit externe
– Réalisé par un prestataire français (organisme de certification accrédité COFRAC ou équivalent)
– Fréquence : tous les 3 ans pour ISO 27001 + audit intermédiaire de surveillance chaque année
– Audit RGPD : tous les 2 ans ou à la demande en cas de modification majeure des traitements
• Gestion des non-conformités
– Enregistrement dans le registre des non-conformités (format tableur ou GED)
– Chaque NC fait l’objet d’un plan d’action avec responsable désigné et échéancier
• Revue de la PSSI
– Révision formelle : annuelle ou après tout incident majeur
– Communication des mises à jour à tous les collaborateurs via newsletter interne et formation flash

4 Organisation de la sécurité

4.1 Schéma des responsabilités

Rôle

– Directeur Général (Adel B)
• Arbitrage budgétaire et validation des orientations stratégiques de la sécurité
• Validation finale de la PSSI et des plans de traitement des risques
– RSSI (Caulin L)
• Pilotage opérationnel du SMSI (Système de Management de la Sécurité de l'Information)
• Animation de la gestion des risques, incidents et audits
• Élaboration et suivi des indicateurs de performance et de risque
– DPO (interne ou prestataire externe)
• Mise en œuvre des solutions techniques validées par le RSSI
• Supervision de l'exploitation quotidienne (réseau, serveurs, postes de travail)
• Coordination avec les prestataires externes (cloud, audit)
• Garantie de la conformité RGPD : registres de traitement, DPIA, gestion des droits des personnes
– Pilotes de domaine (développement, infrastructure, support, production)
• Responsables de la sécurité au niveau de leur périmètre métier
• Veillent à l'application des procédures et au respect des bonnes pratiques
– Collaborateurs
• Respect des procédures d'accès, des consignes de sécurité et des obligations RGPD
• Signalement immédiat de tout incident ou anomalie

4.2 Comité de pilotage sécurité

Composition

– Adel B (Direction)
– Caulin L (RSSI)
– DPO (interne ou externe)
– DSI
– Un pilote de domaine par fonction critique

Missions

– Valider les politiques, les procédures et les plans d'action sécurité
– Arbitrer les choix technologiques et budgétaires
– Suivre l'état des risques et le tableau de bord (KPI/KRI)
– Examiner les résultats d'audits internes et externes
– Coordonner la communication sur les incidents majeurs

Fréquence des réunions

– Proposition : semestrielle (possibilité de passer à trimestrielle selon niveau de risque)

4.3 Processus de revue et d’escalade

4.3.1 Revue périodique

– Revue mensuelle par le RSSI : mise à jour du registre des risques, suivi des indicateurs (MTTD, MTTR, correctifs, incidents)
– Revue semestrielle par le Comité de pilotage : état d’avancement des plans d’actions, audits, conformité RGPD et ISO 27001
– Revue annuelle en revue de direction : bilan global, ajustement de la PSSI et objectifs pour l’année suivante

4.3.2 Gestion des incidents et d’escalade

– Détection et signalement : tout collaborateur informe le RSSI sous 2 heures dès détection d’un incident de sécurité
– Classification de l’incident (A – critique, B – majeur, C – mineur) par le RSSI dans un délai de 4 heures
– Traitement
• Niveau A : réunion d’urgence du Comité de pilotage (sous 24 h), notification aux autorités compétentes (le cas échéant)
• Niveau B : plan d’action correctif piloté par le RSSI, reporting hebdomadaire au Comité
• Niveau C : traitement dans le cadre du processus de maintenance classique
– Clôture et retour d’expérience : rapport d’incident, mise à jour des procédures et formation éventuelle du personnel

5 Gestion des actifs & classification des données

5.1 Inventaire des actifs

Un registre des actifs est tenu à jour par le RSSI, en collaboration avec le DSI et les pilotes de domaine. Il recense notamment :

• Matériels

- Serveurs hébergeant l'application e-commerce CovY (physiques ou virtuels)
- Équipements réseau (firewalls, routeurs, switchs)
- Postes de travail fixes et portables des collaborateurs mis à jour automatiquement
- Terminaux mobiles (smartphones, tablettes) utilisés en télétravail
- Périphériques de sauvegarde (NAS, bandes, cloud backup)

• Logiciels et composants applicatifs

- Système de gestion de base de données (MySQL, PostgreSQL, etc.)
- Plateforme e-commerce (front-end, back-office, API)
- Environnements de développement et frameworks (IDE, bibliothèques, conteneurs Docker)
- Solutions de sécurité (antivirus, EDR, WAF, VPN)
- Outils de monitoring, de journalisation et de sauvegarde

• Données

- Informations personnelles clients (identité, coordonnées, historique d'achats)
- Données de paiement (tokenisation, logs de transactions)
- Journalisation des accès et des incidents (logs serveurs, pare-feu, VPN)
- Code source et configurations d'infrastructure (IaC, scripts)

5.2 Criticité et niveaux de classification

Chaque actif est évalué selon son impact sur la continuité de service, la confidentialité des données et l'image de CovY. Quatre niveaux de classification sont définis :

• Niveau 1 – Public

Données et documents destinés à diffusion externe sans risque (présentation marketing, mentions légales).

• Niveau 2 – Interne

Informations à usage interne à l'entreprise (procédures internes, notes de service, planning d'équipe).

• Niveau 3 – Confidentiel
Données sensibles nécessitant une protection renforcée :
– Informations personnelles clients (RGPD)
– Codes sources non publiés
– Comptes et accès administrateurs
– Plan de continuité d'activité (PCA)

• Niveau 4 – Restreint
Actifs critiques dont la divulgation ou la perte entraîne une interruption majeure de service ou un préjudice financier important :
– Clés de chiffrement privées
– Accès root/root ssh
– Bases de données de production intégrales
– Plan de reprise d'activité (PRA)

Les règles de traitement par niveau :
– Niveau 1 : pas de chiffrement, partage libre.
– Niveau 2 : authentification standard, sauvegarde régulière.
– Niveau 3 : chiffrement en transit et au repos, accès restreints, contrôle d'audit.
– Niveau 4 : isolation réseau, MFA obligatoire, journalisation détaillée, double validation des actions critiques.

5.3 Propriétaires et responsables des actifs
Pour chaque actif et chaque niveau de classification, un propriétaire et un responsable opérationnel sont désignés :
• Propriétaire de l'actif
– Rôle stratégique, décide des règles d'usage et de protection
– Exemples :
• Données clients : DG (Adel B)
• Code source : Responsable R&D / Pilote développement
• Infrastructure réseau : DSI

• Responsable opérationnel
– Met en œuvre et maintient les mesures de sécurité quotidiennes
– Exemples :
• Serveurs et stockage : Administrateur système (DSI)
• Outils de sauvegarde et de journalisation : Pilote Infrastructure
• Gestion des accès et identités : RSSI (Caulin L)

• DPO (interne ou prestataire)
– Propriétaire fonctionnel des traitements de données personnelles
– Garant du respect des droits des personnes et des obligations RGPD

Le registre des actifs doit préciser pour chaque élément :
• Désignation et description
• Niveau de classification
• Propriétaire et responsable opérationnel
• Localisation physique ou logique
• Échéance de révision de la classification (au moins annuelle)

Cette organisation garantit une traçabilité claire, un partage de responsabilités structuré et une protection adaptée au contexte full remote de CovY.

6 Contrôle d’accès & authentification

6.1 Politique de gestion des comptes et habilitations

6.1.1 Création, modification et suppression de comptes

• Toute demande de création ou de modification d’habilitation est formulée via le portail interne ou par ticket, validée par le RSSI.
• Les comptes sont liées à une identité unique (« no shared accounts »).
• Les comptes inactifs depuis plus de 30 jours sont automatiquement désactivés.
• Les suppressions de comptes interviennent dans les 24 h suivant la fin de contrat ou le changement de fonction, sur instruction du service RH ou du RSSI.

6.1.2 Gestion des droits et des habilitations

• Attribution des droits selon un catalogue de profils standardisés (dev, infra, support, finance, marketing).
• Chaque accès critique (base de données production, consoles d’administration, coffre-fort de mots de passe) fait l’objet d’une validation spécifique du RSSI ou du DPO selon la nature du risque.
• Revue trimestrielle des habilitations : le RSSI pilote un process de vérification avec les pilotes de domaine pour retrait des droits non justifiés.

6.2.2 Politique de mots de passe

• Longueur minimale : 12 caractères, incluant majuscules, minuscules, chiffres et symboles.
• Rotation tous les 90 jours ; historique des 5 derniers mots de passe conservé pour empêcher la remise en service.
• Verrouillage automatique après 5 échecs de connexion consécutifs : durée de blocage 15 minutes.
• Stockage chiffré des mots de passe via un gestionnaire de secrets (keepass).
• Interdiction d’écrire ou de partager les mots de passe par email ou messagerie non chiffrée.

6.3 RBAC et principe du moindre privilège

6.3.1 Modèle RBAC (Role-Based Access Control)

• Définition d’un référentiel de rôles (Administrateur, Développeur, Support, Analyste, etc.) avec droits clairement documentés.
• Toute demande d’accès à un rôle est soumise à validation du pilote de domaine et du RSSI.
• Les rôles sont alignés avec les procédures ISO 27001 et les exigences RGPD pour les traitements de données personnelles.

6.3.2 Principe du moindre privilège

• Les utilisateurs ne reçoivent en production que les droits strictement nécessaires à leurs missions.

• Pour toute élévation temporaire de privilèges, une demande formelle est déposée, validée, puis révoquée automatiquement à échéance.

• Mise en place de « break-glass accounts » pour situations d’urgence : comptes réservés, usage journalisé et revu par le RSSI.

6.3.3 Séparation des fonctions

• Aucune personne ne peut à la fois demander, approuver et exécuter une même opération critique.

• Les actions sensibles (déploiements, modifications de configuration, accès aux clés de chiffrement) sont toujours soumises à une double validation (pilote de domaine + RSSI).

7 Sécurité réseau & communications

7.1 Topologie réseau et segmentation

• Vue d’ensemble

– Réseau divisé en zones logiques distinctes : Front-office (DMZ), back-office, base de données, management, environnements de développement et de test.

– Chaque zone isolée par des VLANs et soumise à des règles de filtrage strictes.

• Segmentation interne

– DMZ : héberge les serveurs web/applications accessibles depuis Internet, protégés par pare-feu périmétrique.

– Zone interne : uniquement accessible depuis la DMZ et via le réseau de management (bastion).

– Zone base de données (vlan 30) : fermée à tout accès direct public, seuls les serveurs applicatifs y accèdent sur ports restreints.

7.2 VPN, pare-feux, IDS/IPS

• VPN

– Accès distant des collaborateurs full-remote via VPN SSL/IPsec avec MFA obligatoire.

– Pas de split-tunneling : tout trafic traverse le réseau d’entreprise pour appliquer les contrôles.

– Journaux de connexion conservés et corrélés dans le SIEM.

• Pare-feux

– Pare-feu périmétrique Next-Gen en entrée/sortie pour filtrage applicatif (niveau 7), inspection HTTPS et blocage de menaces connues.

– Pare-feux internes (« micro-segmentation ») entre chaque zone pour limiter les mouvements latéraux.

– Mise à jour des règles et des signatures au moins mensuellement, revue semestrielle des politiques.

• IDS/IPS

– Déploiement d’un IDS réseau (signature + comportemental) sur les liens DMZ ↔ App et App ↔ BD, alertant le SOC.

– IPS activé en mode inline pour bloquer automatiquement les attaques critiques (ex : tentatives d’injection, balayages de ports).

– Processus de tuning continu : analyse des faux-positifs, mise à jour des règles de détection, feed-back sur incidents.

– Intégration des alertes dans la console SIEM pour corrélation avec les logs des firewalls et serveurs.

7.3 Chiffrement des communications

• Chiffrement des flux externes

– TLS 1.2/1.3 pour tous les accès web (HTTP Strict Transport Security, certificats validés par une AC reconnue).

– Renouvellement automatique des certificats via AC interne ou service de type Let’s Encrypt.

• Chiffrement interne

– Chiffrement IPsec ou TLS pour les communications sensibles entre zones (app → BD, management → serveurs).

– SSH (version 2) pour l’administration : ciphers AES-256, clés ECDSA 256 bits, MFA sur jump-hosts.

• Chiffrement des échanges machine-à-machine

– Mutual TLS pour les API internes et externes, avec vérification stricte de la chaîne de confiance.

– Rotation régulière des clés et certificats, gestion centralisée via un PKI interne ou vault sécurisé.

• Protocoles annexes

– SMTP opportuniste avec STARTTLS pour la messagerie, S/MIME ou PGP pour le chiffrage de bout en bout si nécessaire.

– DNSSEC pour garantir l’intégrité des résolutions DNS critiques (services de paiement, sous-domaines e-commerce).

8 Sécurité des systèmes & des services

8.1 Standards de configuration

8.1.1 Baseline et référentiels

• Adoption de référentiels reconnus (CIS Benchmarks, ANSSI, STIG) pour chaque OS (Windows, Linux, macOS) et chaque type de serveur (web, base de données, applicatif).
• Modèles de configuration validés par le RSSI et mis à disposition via le gestionnaire de configuration (Ansible, Puppet, Chef).
• Versioning des playbooks et scripts de déploiement dans le dépôt Git central, avec revue de code par un second ingénieur.

8.1.2 Postes de travail

• Image standardisée intégrant :
– Antivirus/EDR, chiffrement disque (BitLocker, LUKS), pare-feu local configuré.
• Politique de verrouillage automatique (écran verrouillé après 5 min d'inactivité).
• Installation contrôlée des logiciels : catalogue validé, installation via SCCM, interdiction des droits Administrateur local.

8.1.3 Serveurs

• Configuration minimale (services et ports) : seule l'infrastructure nécessaire au rôle est installée et activée.
• Journalisation système (auditd, Windows Event) et envoi centralisé vers le SIEM.
• Agents de monitoring (CPU, RAM, SSH uptime) et alerting sur seuils critiques.

8.2 Gestion des correctifs et des antivirus

8.2.1 Processus de gestion des correctifs

• Inventaire automatisé des versions logicielles et correctifs applicables via un outil dédié (WSUS, Satellite, Spacewalk, etc.).
• Priorisation : sécurité critique (CVSS ≥ 7.0) appliquée sous 72 h, correctifs majeurs sous 30 jours, correctifs mineurs selon planning semestriel.
• Phase de tests en environnement dev/test avant déploiement en production, puis déploiement piloté en fenêtres de maintenance validées par le Comité de pilotage sécurité.
• Rollback documenté et plan de reprise en cas d'incident suite à un correctif.

8.2.2 Protection antivirus et EDR

• Déploiement d’une solution EDR centralisée sur tous les endpoints et serveurs.
• Signature et moteur comportemental mis à jour automatiquement, au moins quotidiennement.
• Alertes critiques escaladées au SOC / RSSI, investigations sur faux-positifs et tuning continu.
• Procédure de quarantaine et de nettoyage automatique des fichiers malveillants, rapports mensuels des incidents détectés.

8.3 Durcissement et inventaire des services exposés

8.3.1 Durcissement des services

• Désactivation des protocoles obsolètes (SMBv1, TLS < 1.2, Telnet, RDP non sécurisé) et des composants non utilisés (LDAP simple bind, FTP non chiffré).
• Mise en œuvre de headers de sécurité sur serveurs web (HSTS, CSP, X-Frame-Options, X-Content-Type-Options).
• Séparation des environnements : production, recette, dev/test, sans accès direct cross-environnements.

8.3.2 Inventaire des services exposés

• Scan mensuel automatisé (Nessus, OpenVAS, Qualys) de l’ensemble des IP publiques et des plages internes critiques.
• Registre des services exposés maintenu par l’équipe infrastructure : type de service, version, port, date de dernier scan et état de mise à jour.
• Analyse des vulnérabilités détectées, plan de traitement avec priorisation (CRITICAL, HIGH, MEDIUM, LOW) et suivi des tickets jusqu’à clôture.
• Revue trimestrielle avec le RSSI pour validation des risques résiduels et ajustement du périmètre de scanning.

9 Analyse des risques & gestion des vulnérabilités

9.1 Méthodologie d’analyse des risques

• Cadre et référentiels

– Adoption conjointe des normes ISO 27005 et de la méthode EBIOS pour structurer l’analyse.

– Intégration des exigences RGPD et des contraintes métier propres à l’activité e-commerce de CovY.

• Processus d’analyse

1. Inventaire et cartographie des actifs critiques (cf. section 5).
2. Identification des scénarios de menace : acteurs (hackers, malveillances internes, erreurs humaines), vecteurs d’attaque, vulnérabilités.
3. Évaluation du risque : probabilité d’occurrence et impact business (financier, réputation, conformité).
4. Priorisation des risques selon matrices personnalisées (échelle 1–5 pour probabilité et impact).
5. Définition et mise en œuvre des mesures de traitement : éviter, réduire, transférer, accepter.
6. Suivi et révision : revue annuelle ou à chaque changement majeur (nouvelle fonctionnalité, migration, fusion).

9.2 Outils de scan de vulnérabilités

• Outils automatisés

– Scanners réseau et systèmes : Nessus, OpenVAS, QualysGuard.

– Scanners applicatifs : OWASP ZAP, Burp Suite Professional pour détection des failles web (OWASP Top 10).

• Processus de scan

1. Planification : définition du périmètre (IP, domaines, applications), calendrier et fenêtre de tests.
2. Exécution : scans internes hebdomadaires, scans externes mensuels, hors pics d’activité.
3. Consolidation des résultats dans le SIEM pour corrélation avec logs et détections IDS/IPS.
4. Analyse et classification des vulnérabilités selon CVSS v3.1 (Critical ≥ 9.0, High 7.0–8.9, Medium 4.0–6.9, Low < 4.0).

5. Élaboration d’un plan de remédiation : assignation aux pilotes de domaine, délais C0 (72 h), C1 (30 j), C2 (6 mois).

9.3 Planification et suivi des pentests
• Périmètre et périodicité
– Pentest infrastructure et réseau : annuel, boîte grise, couvrant DMZ, VPN, bastions.
– Pentest application e-commerce : semestriel, tests fonctionnels et API, injection, authentification, logique métier.
– Red team exercise (simulations d’attaque globales) : tous les 18 mois, avec objectifs définis.
• Sélection du prestataire
– Qualification selon critères : certifications (OSCP, CISSP), expérience e-commerce, respect NDA et code éthique.
– Cahier des charges précisant objectifs, méthodologie (PTES, OSSTMM), modalités de restitution.
• Déroulement

1. Kick-off meeting : validation du scope, modes (black box / grey box), fenêtres de test.
2. Tests d’intrusion : collecte d’informations, exploitation, escalade de privilèges, maintien d’accès.
3. Rapport détaillé : vulnérabilités trouvées, preuves de concept, classification CVSS, recommandations de remédiation et durcissement.
   • Suivi et validation
   – Création de tickets de remédiation dans le système ITSM, attribution aux responsables techniques avec SLA défini.
   – Re-test ciblés sur les failles critiques une fois les correctifs appliqués.
   – Présentation des résultats et du closing report au Comité de pilotage sécurité pour validation du risque résiduel.

10 Protection des données & vie privée

10.1 Chiffrement au repos et en transit

• Chiffrement au repos

– Bases de données et volumes de stockage chiffrés (AES-256 GCM) via mécanismes natifs (BitLocker).

– Clés de chiffrement gérées dans un coffre fort matériel ou logiciel (Vault) avec séparation des rôles (séparation des opérations de chiffrement et d'administration).

– Chiffrement des sauvegardes et des snapshots avant export ou archivage, contrôle d'accès restreint sur les copies.

• Chiffrement en transit

– TLS 1.2/1.3 obligatoire pour tous les échanges HTTP(S), API REST/GraphQL et flux internes critiques.

– Utilisation de suites de chiffrement robustes (ECDHE, AES-GCM) et désactivation des protocoles obsolètes.

– Chiffrement des tunnels VPN (IPsec ou SSL) avec authentification mutuelle et MFA pour les accès administratifs.

– SSH version 2 pour l'administration à distance, ciphers AES-256 et clés ECDSA ≥256 bits.

10.2 Politique de sauvegarde et restauration

• Stratégie de sauvegarde

– Modèle 3-2-1 : 3 copies des données, sur 2 supports différents, 1 copie hors site (cloud ou site distant).

– Sauvegardes incrémentielles journalières, sauvegarde complète hebdomadaire.

– Chiffrement et signature des sauvegardes pour garantir intégrité et confidentialité.

• Plan de restauration

– Procédures documentées pour restauration partielle (fichiers, bases) et restauration complète (site, VM).

– Fenêtres de test trimestrielles de restauration sur environnement isolé, validation des RPO (Recovery Point Objective) et RTO (Recovery Time Objective).

– Inventaire des jeux de sauvegarde et de leur date, suivi des rapports de succès/erreur et alerting automatisé en cas d'échec.

• Conservation et purge

– Durée de rétention définie selon criticité : courts termes (30 jours), moyen terme (1 an), long terme réglementaire (5 ans).

– Politique de purge automatique et sécurisée (suppression irréversible, écrasement).

10.3 Conformité RGPD (DPO, registre des traitements, DPIA)

• Gouvernance et rôles

– Délégué à la protection des données (DPO) désigné, point de contact interne/externe pour toutes les questions RGPD.

– Comité vie privée réunissant DPO, RSSI, juriste et représentant métier pour arbitrer les traitements à risque.

• Registre des activités de traitement

– Recensement exhaustif des traitements (finalité, catégories de données, durée de conservation, destinataires, base légale).

– Mise à jour continue via un outil collaboratif, revue annuelle et avant toute mise en production d'un nouveau service.

• Analyse d'impact relative à la protection des données (DPIA)

– DPIA obligatoire pour tout traitement à haut risque (profilage, géolocalisation, gestion des paiements, données sensibles).

– Méthodologie structurée : description du traitement, évaluation de la nécessité/proportionnalité, identification et réduction des risques pour les droits et libertés des personnes.

– Validation du DPIA par le DPO et le RSSI, suivi des mesures correctives et des recommandations.

• Droits des personnes et gestion des incidents

– Processus clair et simple pour l'exercice des droits (accès, rectification, effacement, portabilité), délai de réponse maximal 1 mois.

– Notification des violations de données personnelles au CNIL et aux personnes concernées sous 72 heures, enrichissement du registre des incidents.

– Formation et sensibilisation régulière des équipes métier sur les bonnes pratiques RGPD (minimisation, consentement, privacy by design).

11 Plan de continuité d’activité (PCA) & reprise (PRA) adapté au full remote

11.1 Stratégies de sauvegarde hors site pour un environnement 100 % remote

• Modèle 3-2-1 étendu aux postes distants

– Agents de sauvegarde installés sur chaque endpoint (laptop, poste fixe à domicile) : 1 cache local chiffré + 1 copie sur cloud principal + 1 copie sur cloud secondaire ou second datacenter.

– Chiffrement AES-256 au repos et TLS 1.2+ en transit.

– Snapshots immuables (WORM, Object Lock AWS S3/Azure Blob) pour prévenir la suppression ou le chiffrement malveillant.

• Réplication temps-réel ou quasi-temps-réel

– Base de données centralisées et documents critiques (SharePoint, OneDrive, Google Workspace) répliqués dans deux régions géo-distinctes.

– Services IaaS/PaaS : sauvegardes automatisées de VM et conteneurs sur deux ensembles de storage indépendants.

• Catalogage, inventaire et accès

– Registre centralisé (GRC) des jeux de sauvegarde par utilisateur ou service : horodatage, contenu, emplacement, responsable.

– Gestion des accès via IAM (RBAC) et double authentification pour toute opération de restauration ou destruction.

– Workflows d’autorisation digitalisés (ticketing, approbation via Teams/Slack).

11.2 Scénarios de reprise et RTO/RPO en full remote

• Agenda des contacts et planning

– Liste centralisée (Teams/SharePoint) des référents PCA : nom, rôle, fuseau horaire, coordonnées, plages de disponibilité.

– Notifications automatiques (Teams/Email/mobile push) en cas de déclenchement PCA.

• Business Impact Analysis (BIA)

– Cartographie des processus métiers critiques accessibles à distance (CRM cloud, ERP SaaS, outils de collaboration).

– Dépendances clés : accès VPN, MFA, réseau domestique, fournisseurs cloud.

– Classification des services en tiers 1–4 avec RTO/RPO spécifiques :

• Tier 1 (collaboration, messagerie, CRM) : RTO ≤ 1 h, RPO ≤ 15 min

• Tier 2 (intranet, portail RH) : RTO ≤ 4 h, RPO ≤ 1 h

• Tier 3–4 (services supports, archivage) : RTO ≤ 24 h, RPO ≤ 4 h

• Stratégies de reprise par niveau

– Hot site cloud (Tier 1) : environnements SaaS multi-AZ, bascule DNS/AD automatique, configuration VPN globale.
– Warm site virtuel (Tier 2) : abonnements cloud pré-payés, templates IaC (Terraform/ARM) pour déploiement automatisé, restauration snapshots.
– Cold site dématérialisé (Tier 3–4) : espace de ressources cloud alloué à la volée, scripts de provisioning semi-automatiques, possibilité de shipping de laptops préconfigurés.
• Playbooks détaillés
– Séquenceur d'actions : 1. Active Directory/Azure AD, 2. VPN & accès MFA, 3. Bases de données, 4. Applications métiers, 5. Postes utilisateurs.
– Rôles et responsabilités précisés (PCA Manager, Admin Cloud, SecOps, Support Utilisateurs).
– Modèles de communications (Email, Teams, SMS) à diffuser aux collaborateurs.

11.3 Tests, exercices et amélioration continue en full remote
• Fréquence et modalités
– Tabletop trimestriels 100 % à distance (Teams/Zoom) : revue des processus, communications, rôles.
– Tests annuels de bascule cloud (failover) : chaque service Tier 1 validé par 1 h de bascule, connexion à l'environnement de secours, validation des RTO/RPO.
– Drills semestriels ciblés (VPN, MFA, restauration fichiers) : montée en charge virtuelle et validation des temps de restauration.
• Reporting et retours d'expérience
– Rapport post-exercice partagé sur l'intranet : indicateurs RTO/RPO mesurés, points d'amélioration, non-conformités.
– Comité PCA/PRA (RSSI, DPO, DSI remote ops) : revue des rapports, arbitrage des actions correctives, mise à jour du plan sous 30 jours.
• Sensibilisation et formation
– Webinars annuels pour équipes distantes : procédures de déclenchement, restau via portail self-service, communication de crise.
– Fiches réflexes et vidéos hébergées en accès libre (intranet/mobile app) : checklist pré-incident et post-incident pour collaborateurs full remote.
– Simulations d'appel d'urgence : test de la chaîne d'alerte téléphonique/SMS pour s'assurer de la couverture des collaborateurs partout.

12 Sensibilisation, formation & culture sécurité

12.1 Programme de formation remote

• Plateforme e-learning centralisée

– Catalogues de modules interactifs (vidéos, quiz, serious games) couvrant les fondamentaux : gestion des mots de passe, phishing, usage du VPN etc...

– Accès single sign-on via l'Azure AD ou l'IdP interne pour assurer traçabilité et complétude.

• Parcours adaptatifs et obligatoires

– Parcours "Nouveaux arrivants" (2 h de formation initiale à compléter dans les 15 jours).

– Parcours "Perfectionnement" annuel (1 h obligatoire + 2 h optionnelles selon métiers).

– Modules "Spécial RSSI" pour l'encadrement (gouvernance, pilotage du risque).

• Suivi et KPI

– Taux de complétion mensuel, temps moyen passé, score moyen aux quiz.

– Relances automatiques par mail si échéance dépassée.

– Reporting trimestriel au RSSI des formations des employés

12.2 Phishing tests et campagnes de communication

• Campagnes de phishing simulé

– Outils dédiés (KnowBe4, Cofense, Gophish) pour envoi bimensuel de mails "pièges" ciblant différents profils (finance, RH, IT).

– Scénarios variés : pièces jointes malveillantes, liens vers faux portails, usurpation de collègues.

– Mesure des indicateurs : taux d'ouverture, taux de clic, taux de signalement.

• Feedback et coaching

– Alertes automatiques aux personnes ayant cliqué, redirection vers un module de remédiation court (1–3 mn).

– Séances de coaching collectif mensuelles pour les personnes ayant cliqués

• Campagnes de communication régulières

– Newsletters mensuelles "Le coin sécurité" (études de cas réels, astuces, nouveautés).

– Affichage digital dans les écrans communs (hall, cafétéria) avec rappel des bonnes pratiques.

– Challenges ludiques (quiz, concours de mots de passe les plus forts) avec récompenses symboliques.

12.3 Guides pour poste de travail à domicile

• Kit de démarrage sécurisé

– Checklist de configuration : mises à jour OS/applications, antivirus activé, chiffrement disque, pare-feu personnel.

– Configuration du réseau Wi-Fi : WPA3 ou WPA2-AES, mot de passe complexe, désactivation du WPS, segmentation IoT si possible.

– Installation et usage du VPN d’entreprise (always-on, kill-switch activé).

• Bonnes pratiques d’usage

– Séparation vie pro/vie perso : comptes distincts, navigateurs dédiés, stockage chiffré des fichiers d’entreprise.

– Interdiction de partager le poste ou l’accès aux enfants/autres occupants.

– Gestion des impressions et scans : suppression régulière, stockage chiffré si documents sensibles.

• Supports et assistance

– Guide PDF et vidéo tutoriels accessibles via l’intranet et l’application mobile interne.

– Hotline dédiée téléphonique et chat Teams pour support sécurité (SLA 4 h en journée ouvrée).

– FAQ évolutive enrichie des retours terrain et incidents remontés par le SOC.

13 Mise en œuvre, suivi, audit & amélioration continue

13.1 Indicateurs de sécurité (KPI, KRI)

• KPI (Key Performance Indicators) – Mesurent l'efficacité des dispositifs
– Taux de conformité des correctifs (patch compliance rate)
– Nombre et délai moyen de traitement des incidents de sécurité
– Temps moyen de détection (MTTD) et de réponse (MTTR) aux incidents
– Pourcentage d'actifs inventoriés et scannés périodiquement
– Taux d'échecs de sauvegarde et délais de restauration
– Niveau de sensibilisation (taux de complétion des formations, clics au phishing)
• KRI (Key Risk Indicators) – Anticipent l'évolution du profil de risque
– Volume de vulnérabilités critiques/Patch backlog
– % d'activités métiers sans plan de continuité validé
– Nombre d'écarts majeurs relevés en audit
– Taux d'utilisateurs avec droits excessifs
– Indicateurs de menace externe (tentatives d'intrusion, campagnes ciblées)

13.2 Processus d'audit interne et revue de la PSSI

• Audit interne
– Plan d'audit annuel aligné ISO 27001: périmètre, ressources, planning
– Check-lists par domaine (contrôles d'accès, sauvegarde, monitoring, PCA/PRA…)
– Réalisation : collecte de preuves, entretiens, tests d'efficacité des contrôles
– Rapport d'audit détaillé avec observations, écarts classés (mineur/mineur/critique)
• Revue de la PSSI
– Fréquence : au minimum annuelle ou après tout incident majeur ou évolution réglementaire
– Pilotage par le Comité Sécurité (RSSI, DPO, IT, métiers)
– Ordre du jour : retours d'audit, indicateurs KPI/KRI, état d'avancement des plans d'action, nouveaux risques
– Validation et mise à jour formalisée de la PSSI, communication aux parties prenantes

13.3 Gestion des non-conformités et plans d'action

• Identification et classification
– Non-conformités détectées via audits, contrôles automatisés, incidents ou retours tiers
– Criticité définie selon impact métier et niveau de risque (mineure, majeure,

critique)
• Processus de traitement
– Ouverture d’un ticket dans l’outil de GRC/ITSM avec description, priorité, responsable et échéance
– Élaboration d’un plan d’action CAPA : cause racine, mesures correctives et préventives, ressources, jalons
• Suivi et clôture
– Revues périodiques en comité de pilotage PCA/PRA ou Comité Sécurité
– Reporting consolidé des statuts (ouvert, en cours, fermé) et respect des échéances
– Validation finale : preuves de déploiement des actions, tests de vérification
• Boucle d’amélioration
– Capitalisation des retours d’expérience pour enrichir la PSSI, les procédures et les formations
– Publication de fiches « leçons apprises » et partage lors de comités métier
– Mise à jour continue des référentiels et des contrôles automatisés.