REGISTRE DES INCIDENTS DE SÉCURITÉ

Document de traçabilité conforme NIS2 Art. 23 et RGPD Art. 33 — Format A4 paysage

Entreprise : *[Nom de l'entreprise]*

Responsable : *[Nom RSSI / DPO]*

Période : *[Trimestre / Année]*

Version : *[v1.0]*

NIS2 — RGPD CONFORME

NIS2 Art. 23 : Notification obligatoire à l'ANSSI dans les 24h (alerte précoce) puis 72h (notification) pour les entités essentielles/importantes

RGPD Art. 33 : Notification à la CNIL dans les 72h pour toute violation de données personnelles

RGPD Art. 34 : Information des personnes concernées si risque élevé

Conservation : Ce registre doit être conservé minimum 3 ans

Accès : Restreint — RSSI, DPO, Direction

N°	Date détect.	Heure détect.	Type d'incident	Sév. (1-4)	Description	Systèmes impactés	Actions immédiates	Responsable	Statut	Date clôture	Retex / Mesures correctives	Notif. CNIL/ ANSSI
EX.1	15/03/2026	09:32	Phishing — Compte email compromis	**2**	Un collaborateur a cliqué sur un lien de phishing. Son compte email a envoyé 2000 spams à ses contacts en 3h.	Serveur Exchange — 1 compte utilisateur	Révocation du token OAuth, réinitialisation du MDP, activation MFA, analyse de la boîte envoyée	J. Dupont (RSSI)	✓ CLÔTURÉ	17/03/2026	Formation anti-phishing obligatoire pour tous — Mise en place du filtre DMARC/ DKIM	Non requise (données int.)
1				○					—			
2				○					—			
3				○					—			
4				○					—			
5				○					—			
6				○					—			
7				○					—			
8				○					—			
9				○					—			
10				○					—			

TYPES D'INCIDENTS COURANTS

- Ransomware
- Phishing / Spear-phishing
- Fuite de données
- Intrusion / Accès non autorisé
- Déni de service (DDoS)
- Malware / Virus / Spyware
- Ingénierie sociale / Vishing
- Perte / vol matériel
- Erreur humaine / Configuration
- Incident physique

MATRICE DE SÉVÉRITÉ

SEV. 1 — CRITIQUE	SI arrêté, ransomware actif, fuite massive. Réponse : 15 min. Escalade direction + ANSSI.
SEV. 2 — ÉLEVÉ	Intrusion confirmée, vol de données avéré. Réponse : 1h. Escalade RSSI + DPO.
SEV. 3 — MODÉRÉ	Malware isolé, phishing réussi. Réponse : 4h. Escalade RSSI + IT.
SEV. 4 — FAIBLE	Tentative bloquée, alerte isolée. Réponse : 48h. IT uniquement.

Légende statut : **OUVERT** · **EN COURS** · **CLÔTURÉ**

INSTRUCTIONS DE TENUE DU REGISTRE

- **Ouverture :** Ouvrir une entrée dès la détection ou le signalement d'un incident, même si non confirmé. Ne pas attendre la qualification.
- **Description :** Décrire précisément les symptômes observés, les systèmes concernés, les données potentiellement affectées et la chronologie.
- **Sévérité :** Utiliser la matrice de sévérité (colonne gauche). La réévaluer en cours d'incident si la situation évolue.
- **Actions :** Documenter toutes les actions prises avec leur horodatage dans le champ "Actions immédiates".
- **Notification CNIL :** Obligatoire si données personnelles concernées (RGPD Art. 33). Délai : 72h. URL : notifications.cnil.fr
- **Notification ANSSI :** Obligatoire pour les entités essentielles/importantes (NIS2 Art. 23). Délai : 24h alerte précoce, 72h notification.
- **Retex :** Remplir la colonne Retex dans les 7 jours suivant la clôture. Capitaliser sur les leçons apprises.
- **Conservation :** Ce registre doit être conservé minimum 3 ans, stocké de manière sécurisée, avec accès restreint (RSSI, DPO, Direction).
- **Audit :** Révision trimestrielle du registre par le RSSI. Présentation des indicateurs au COMEX semestriellement.
- **Confidentialité :** Ce document est confidentiel. Ne pas partager en dehors des personnes habilitées sans anonymisation préalable.