Modèles de rapport d'incident NIS2 — Pack article 23

Toutes les étapes du signalement des incidents importants au titre de NIS2, en formulaires prêts à déposer : l'alerte précoce à 24 heures, la notification d'incident à 72 heures, le rapport intermédiaire/d'avancement et le rapport final à un mois — les champs de contenu sont mis en correspondance avec l'article 23(4)(a)–(e) de la directive (UE) 2022/2555, et les critères d'importance du CIR (UE) 2024/2690 sont intégrés aux champs d'évaluation.

Ce PDF est le compagnon d'impression et de revue. Les fichiers de travail sont les formulaires DOCX (à compléter et à déposer via votre portail national) ; une variante Markdown lisible par machine est fournie pour les agents IA. Les trois sont gratuits sur orbiqhq.com/templates/nis2-incident-reporting-pack — sans e-mail requis.

Base juridique : directive (UE) 2022/2555, art. 23(3)–(4) ; règlement d'exécution (UE) 2024/2690 de la Commission. Les lois nationales de transposition peuvent ajouter des champs ou des délais sectoriels plus courts. Ceci n'est pas un avis juridique.

L'échelle de signalement de l'article 23

Étape	Échéance	Ancrage juridique	Contenu obligatoire
Formulaire 1 — Alerte précoce	Dans les 24 heures suivant la prise de connaissance	Art 23(4)(a)	Indiquer si l'incident est soupçonné de résulter d'actes illicites ou malveillants et s'il pourrait avoir un impact transfrontière.
Formulaire 2 — Notification d'incident	Dans les 72 heures suivant la prise de connaissance	Art 23(4)(b)	Mise à jour de l'alerte précoce + évaluation initiale de la gravité et de l'impact + indicateurs de compromission lorsqu'ils sont disponibles. (Prestataires de services de confiance : 24 heures.)
Formulaire 3 — Rapport intermédiaire / d'avancement	Sur demande de l'autorité ; ou à un mois si l'incident est en cours	Art 23(4)(c), (e)	Mises à jour pertinentes du statut ; rapport d'avancement lorsque le rapport final ne peut pas encore clore l'incident.
Formulaire 4 — Rapport final	Dans le mois suivant la notification d'incident	Art 23(4)(d)	Description détaillée incl. gravité et impact ; le type de menace ou la cause racine qui l'a probablement déclenché ; les mesures d'atténuation appliquées et en cours ; l'impact transfrontière le cas échéant.

Le chrono démarre à la **prise de connaissance**, pas à la confirmation de la cause racine. L'alerte précoce est volontairement légère afin que le signalement ne détourne pas de ressources de la réponse — l'article 23(5) oblige le CSIRT à répondre avec des orientations dans les 24 heures suivant l'alerte précoce.

Quand un incident est-il « important » ?

L'article 23(3) fixe le test général : perturbation opérationnelle grave des services ou perte financière pour l'entité, ou dommage matériel ou immatériel considérable pour d'autres personnes. Pour les entités d'infrastructure numérique, de gestion de services TIC et les fournisseurs numériques, le CIR (UE) 2024/2690 (applicable depuis le 7 novembre 2024) rend le test quantitatif — les déclencheurs de l'article 3 incluent une perte financière directe supérieure à 500 000 EUR ou à 5 % du chiffre d'affaires annuel (le montant le plus bas étant retenu), l'exfiltration de secrets d'affaires, un accès non autorisé susceptible de causer une perturbation opérationnelle grave, et les incidents récurrents de même cause racine survenant au moins deux fois en six mois et franchissant collectivement le seuil de perte — plus des seuils par service (p. ex. résolution DNS indisponible pendant plus de 30 minutes).

Où déposer

Vous déposez auprès de votre CSIRT ou de votre autorité compétente via les canaux nationaux. France : l'ANSSI (vérifiez l'état de la transposition et votre canal sectoriel). Allemagne : le portail de signalement du BSI (NIS2UmsuCG en vigueur depuis le 6 décembre 2025). Norvège : NSM et l'autorité sectorielle au titre de la digitalsikkerhetsloven (échelle 24 h / 72 h / un mois, en vigueur depuis le 1er octobre 2025). Entités britanniques : le Cyber Security and Resilience Bill propose une notification initiale à 24 heures et un rapport complet à 72 heures au régulateur et au NCSC. Ces formulaires structurent le contenu une seule fois, pour que le dépôt multi-juridictions soit une transcription, pas une rédaction.

Le pack, formulaire par formulaire

Formulaire	Ce qu'il capture
Formulaire 0 — Entrée du registre des incidents (interne)	La source de vérité unique : horodatage de la prise de connaissance (qui démarre le chrono), classification, évaluation de l'importance, journal des rapports avec les références de l'autorité.

Formulaire	Ce qu'il capture
Formulaire 1 — Alerte précoce	Les deux indications obligatoires + le bloc de contact. À compléter en minutes, pas en heures.
Formulaire 2 — Notification d'incident	Évaluation initiale de la gravité et de l'impact, IoC, critères d'importance remplis, état de la réponse, communication aux destinataires du service.
Formulaire 3 — Intermédiaire / avancement	Mises à jour du statut sur demande, ou le rapport d'avancement qui remplace un rapport final impossible.
Formulaire 4 — Rapport final	Les quatre éléments obligatoires de l'art. 23(4)(d), plus un bloc de retour d'expérience alimentant vos mesures de l'art. 21.

Le signalement prouve que l'incident a été géré ; vos mesures de gestion des risques de l'article 21 prouvent qu'il avait été anticipé. Gardez les deux faces connectées — preuves, contrôles, garanties fournisseurs — dans Orbiq : orbiqhq.com.