

NIS2 Incident Report Templates — Article 23 Pack

All stages of NIS2 significant-incident reporting as ready-to-file forms: the 24-hour early warning, the 72-hour incident notification, the intermediate/progress report, and the one-month final report — content fields mapped to Article 23(4)(a)–(e) of Directive (EU) 2022/2555, with the CIR (EU) 2024/2690 significance criteria built into the assessment fields.

This PDF is the print/review companion. The working files are the DOCX forms (complete and submit through your national portal); a machine-readable Markdown variant ships for AI agents. All three are free at orbiqhq.com/templates/nis2-incident-reporting-pack — no email required.

Legal basis: Directive (EU) 2022/2555, Art 23(3)–(4); Commission Implementing Regulation (EU) 2024/2690. National transposition laws may add fields or shorter sector-specific deadlines. Not legal advice.

The Article 23 reporting ladder

Stage	Deadline	Legal anchor	Mandatory content
Form 1 — Early warning	Within 24 hours of awareness	Art 23(4)(a)	Whether the incident is suspected of being caused by unlawful or malicious acts; whether it could have cross-border impact.
Form 2 — Incident notification	Within 72 hours of awareness	Art 23(4)(b)	Update of the early warning + initial assessment of severity and impact + indicators of compromise where available. (Trust service providers: 24 hours.)
Form 3 — Intermediate / progress report	On authority request; or at one month if the incident is ongoing	Art 23(4)(c), (e)	Relevant status updates; progress report where the final report cannot yet close the incident.
Form 4 — Final report	Within one month of the incident notification	Art 23(4)(d)	Detailed description incl. severity and impact; the type of threat or root cause likely to have triggered it; applied and ongoing mitigation; cross-border impact where applicable.

The clock starts at **awareness**, not at confirmation of root cause. The early warning is deliberately light so that reporting does not divert resources from response — Article 23(5) obliges the CSIRT to respond with guidance within 24 hours of the early warning.

When is an incident 'significant'?

Article 23(3) sets the general test: severe operational disruption or financial loss for the entity, or considerable material or non-material damage to other persons. For digital-infrastructure, ICT-service-management and digital-provider entities, CIR (EU) 2024/2690 (applicable since 7 November 2024) makes the test quantitative — Article 3 triggers include direct financial loss exceeding EUR 500,000 or 5% of annual turnover (whichever is lower), exfiltration of trade secrets, unauthorised access capable of causing severe operational disruption, and recurring same-root-cause incidents twice or more within six months that collectively cross the loss threshold — plus per-service thresholds (e.g. DNS resolution down for more than 30 minutes).

Where to file

You report to your CSIRT or competent authority through national channels. Germany: the BSI reporting portal (NIS2UmsuCG in force since 6 December 2025). Norway: NSM and the sector authority under digitalsikkerhetsloven (24h / 72h / one-month ladder, in force since 1 October 2025). UK entities: the Cyber Security and Resilience Bill proposes a 24-hour initial notification and 72-hour full report to the regulator and NCSC. These forms structure the content once so multi-jurisdiction filing is transcription, not drafting.

The pack, form by form

Form	What it captures
Form 0 — Incident register entry (internal)	The single source of truth: awareness timestamp (starts the clock), classification, significance assessment, report log with authority references.
Form 1 — Early warning	The two mandatory indications + contact block. Complete in minutes, not hours.
Form 2 — Incident notification	Initial severity/impact assessment, IoCs, significance criteria met, response status, service-recipient communication.
Form 3 — Intermediate / progress	Status updates on request, or the progress report that replaces an impossible final report.
Form 4 — Final report	The four mandatory Art 23(4)(d) elements plus a lessons-learned block feeding your Art 21 measures.

Reporting proves the incident was handled; your Article 21 risk-management measures prove it was prepared for. Keep both sides connected — evidence, controls, supplier assurances — in Orbiq: orbiqhq.com.