TechSuit · Incident response

# The NIS2 Incident Reporting Playbook

Your step-by-step 24h / 72h / 1-month CSIRT communication guide and emergency response templates.

## What counts as a ”significant incident”

NIS2 Article 23 only starts its clock once an incident crosses a specific bar. Not every phishing email or failed login attempt triggers a mandatory report - but it's safer to assess against these criteria the moment something looks wrong than to debate it while the clock is already running. Under Article 23(3), an incident is "significant" if either of these is true:

- It **has caused, or is capable of causing, serious operational disruption** of your services, or financial loss for your organisation.
- It **has affected, or is capable of affecting, other people** - customers, partners, the public - by causing considerable material or non-material damage. This includes cross-border impact, where the incident touches people or systems in another member state.

If you're not sure whether an incident meets the bar, treat it as if it does until you've had ten minutes to assess it properly. A false alarm costs you an email. A missed 24-hour window costs you a regulatory finding.

# Stage 1: The 24-hour early warning

**Goal:** notify your competent authority or national CSIRT without undue delay, and in any event within 24 hours of becoming aware of a suspected significant incident.

At this stage you're not expected to have the full picture. You're expected to have picked up the phone (or sent the email) before the 24-hour mark. Flag two things clearly if you know them:

- Whether the incident is suspected to result from **unlawful or malicious acts**.
- Whether it could have a **cross-border impact** on people or systems in another EU member state.

## Early-warning template

Copy this into an email to your competent authority or national CSIRT. Subject line: **[URGENT] Early Warning - Suspected Significant Incident - [Your Organisation Name]**

- **To:** [Competent authority / national CSIRT] **From:** [Name, role, direct phone number]
- **Date/time of awareness:** [DD/MM/YYYY, HH:MM, timezone]
- **Impacted system categories:** [Customer-facing services / Internal systems / Third-party or supplier systems / Personal data stores / OT-industrial control systems - list all that apply, with brief detail]
- **Preliminary threat type:** [Ransomware / Data breach / DDoS / Account compromise / Supply-chain compromise / Unknown, still assessing]
- **Cross-border indicators:** [None identified / Suspected - name the affected member state(s)]
- **Malicious actor suspicions:** [Suspected unlawful or malicious act / Suspected accidental or technical failure / Unknown]
- **Immediate containment actions taken:** [What you've already done, in one or two lines]
- **Next update expected by:** within 72 hours of awareness
- **Reported by:** [Name, role, signature]

## Greece: reporting to the National Cybersecurity Authority (NCSA)

Entities regulated in Greece under Law 5160/2024 report to the **National Cybersecurity Authority (NCSA)**, reachable through its official portal at **cyber.gov.gr**. Two things worth knowing before you're in a crisis:

- **There are two Greek CSIRTs, and only one is yours.** A separate CSIRT operates under the Ministry of National Defence for military and defence-related networks. If you're a commercial NIS2-regulated entity, your channel is the civilian NCSA at cyber.gov.gr, not the defence CSIRT.
- **Pull the current contact details from cyber.gov.gr at the moment you need them**, not from a document you saved months ago. Incident-reporting emails, portal links, and any published encryption keys can change, and confirming the live details takes thirty seconds against the cost of sending a sensitive report to a stale address. We deliberately don't hardcode a specific email address or PGP fingerprint in this guide for that reason - always pull the current channel from the official site itself.

- Open your subject line with **[URGENT]** so it doesn't sit in a triage queue. Reference your organisation's NCSA registration details if you've already registered on the platform.

# Stage 2: The 72-hour incident notification

**Goal:** submit a detailed incident notification within 72 hours of becoming aware, updating your early warning with a severity assessment, indicators of compromise, and any mitigation already applied.

## Incident notification template

- **Organisation:** [Name] **Reference/case number:** [From your early warning] **Report submitted by:** [Name, role]
- **1. Incident overview:** date/time began (best estimate), date/time detected, date/time of the 24-hour early warning
- **2. Severity assessment:** [Low / Medium / High / Critical] and the basis for that rating
- **3. Technical assets affected:** systems, number of endpoints/servers/accounts, network segments involved
- **4. Operational downtime:** services degraded or unavailable, estimated downtime so far, estimated total impact
- **5. Data classification breached (if applicable):** [None identified / Internal-business data / Personal data / Special-category or sensitive personal data / Payment-financial data], and an approximate number of individuals or records affected
- **6. Known indicators of compromise (IoCs):** IP addresses, file hashes, malicious domains/URLs, malware family if identified
- **7. Initial mitigation applied:** what's been done since the early warning
- **8. Next steps and estimated timeline to the final report**
- **Reported by:** [Name, role, signature]

## Stage 3: The one-month final report

**Goal:** submit a final report no later than one month after the 72-hour notification.

The final report is where the incident gets closed out properly, both for the regulator and for your own future defence. It needs to cover:

- A **detailed description of the incident** - root cause, severity, and a full timeline from first compromise to full recovery.
- The **threat actor profile and attack vectors** used, to the extent they could be established.
- The **technical and operational mitigation measures** actually applied, not just planned.
- The **long-term improvements** added to your incident response plan so the same root cause can't repeat.

Treat the final report as a proper post-incident review, not a formality. The organisations that come out of an incident stronger are the ones that turn this document into a real list of fixes, then actually implement them.

# Actionable incident recording sheet

Under Spain's ENS (the incident-management control family, op.exp.7) and ISO 27001, you need more than a report at the end - you need a running log that shows exactly what was done, when, and by whom, while the incident was live. That log is what makes your final report credible and what protects you if a regulator or insurer asks how the investigation was actually run.

| Timestamp | Action taken | Performed by | System/evidence affected | Data integrity check |
|---|---|---|---|---|
| **[DD/MM HH:MM]** | [e.g. Isolated affected endpoint from network] | [Name/role] | [Asset ID or system name] | [Hash/checksum recorded? Y/N] |
| | | | | |
| | | | | |
| | | | | |

Keep this log going from the moment you become aware of the incident until the final report is filed. Three rules make it defensible later:

1. **Every entry gets a timestamp and a name.** "Someone restarted the server" isn't an audit trail.
2. **Preserve evidence before you fix anything you can.** Take a forensic image, export logs, or at minimum record hashes before you patch, wipe, or restart a system - once it's gone, it's gone.
3. **Don't edit past entries.** Add corrections as new rows with a note, the same way you'd handle a financial ledger. A log that's been quietly edited after the fact is worth less than no log at all.

If reading this playbook is the first time you're thinking about where this log would even live, that's the gap worth closing before the next incident, not during it. TechSuit sets up incident logging, tested backups, and the underlying CIS Controls v8.1 baseline that keeps most incidents from reaching "significant" in the first place.

**Book a free 30-minute call** and we'll pressure-test your current incident response plan against these three stages, in plain language.