TEMPLATE P26 · INCIDENT RESPONSE PLAN

# Incident response plan

Prepares the response to incidents affecting an AI system: what is considered an incident, how its severity is classified, who acts, how it is contained and which reports must be checked.

**Fernando García Varela** Version 0.1 (working draft) 16-09-2026 Draft for review

IN THIS DOCUMENT


01 Instructions for use

02 Identification

03 What is considered an incident for this system

04 Severity

05 Roles during the incident

06 Response phases

07 Prepared containment actions

08 Regulatory and contractual reports to be verified

09 Internal escalation

10 Drills

11 Quality criteria

12 Approval and verification

13 Version control



**Legal notice and disclaimer.** SEVEN-G is a reference methodological framework provided "as is" and for information purposes only. It does not constitute legal, regulatory, financial or professional advice, nor does it guarantee compliance with any law or standard. References to general regulation (such as the EU AI Act, the GDPR, DORA or NIS2), to technical standards and to regulation specific to each sector or jurisdiction may be incomplete, may not apply to a particular case or may become out of date as a result of regulatory changes, interpretations or supervisory positions after their consultation date. **Each organisation that uses SEVEN-G is solely responsible for identifying the regulation that applies to it, verifying that it is current and certifying its own regulatory compliance**, with the appropriate qualified advice. This methodology is a generic, free aid shared with the community so that nobody has to start from scratch; each person or organisation can and should adapt it to its own use. It must not be inferred that its legally sensitive parts have been reviewed by legal counsel: those reviews, for each company or sector, are the ultimate responsibility of the company, consultant or organisation that uses it. Although every effort is made to keep it up to date, some regulation may have changed without being reflected here. To the fullest extent permitted by law, the author accepts no responsibility whatsoever for the effects of its application in any organisation or for its full applicability. The methodology does not grant certification of any kind. The author accepts no liability for any use made of this content or for any decisions taken on the basis of it. The data, figures, companies and cases in the examples are fictitious or illustrative.


01

# Instructions for use

| Aspect | Guidance |
|---|---|
| **When it is used** | It is prepared in phase 5 (prerequisite for the P23 sign-off) and approved at the start of phase 6. It is reviewed after each S1 or S2 incident and at each R6. |
| **Who completes it** | AI Operations Owner, with information security, data protection and the AI Risk Owner. |
| **Who verifies it** | AI Office at Lite intensity; AI Auditor at Enterprise intensity. |

| Aspect | Guidance |
|---|---|
| **At which *gate* it is reviewed** | G5 (existence and adequacy) and R6 (currency and results of drills). |
| **Lite versus Enterprise** | Lite may omit the fields marked **(Enterprise)**. The check of regulatory reports (block 8) is never omitted. |
| **Tool** | T08 Nonconformity and incident register. |
| **Relationship** | P17 Human oversight · P18 Security and kill switch · P19 Rollback · P24 Operations manual · P25 Alerts · P27 Incident and change log · documents 35, 37 (Nonconformities and incidents) and 52. |

Rules:

- The **severity criteria, reporting time limits and the full process** are set out in document 37. This plan applies them to the specific system; it does not set its own regulatory time limits.
- This plan is integrated into the company's general incident management process (security, continuity, data protection); it does not create a parallel circuit.
- A serious incident not reported when reporting was required is a **critical** nonconformity (01 §12).
- In case of doubt about severity, the incident is classified at the higher level and reviewed afterwards.

This template does not constitute legal advice. Reporting obligations and their time limits must be verified with legal counsel at the time of the incident (reference consultation date for the framework: September 2026).

02

# Identification

| Field | Content | Guidance |
|---|---|---|
| **Use case code** | | IA-AAAA-NNN (T01). |
| **AI system(s)** | | Identifier in the inventory (T02). |
| **Regulatory classification** | | Prohibited · High risk · Transparency obligations · Minimal risk · Out of scope · Pending classification. |
| **Role of the company in relation to the system** | | Provider · Deployer · Both · To be determined. It determines the reporting obligations (document 34). |

| Field | Content | Guidance |
|---|---|---|
| **Subject to DORA ?** | | Yes · No · To be determined. |
| **Subject to NIS2 (according to national transposition)?** | | Yes · No · To be determined. |
| **Does it process personal data?** | | Yes · No. |
| **Intensity** | | Lite · Enterprise. |
| **Document version** | | |
| **Author** | | Role and name. |
| **Date** | | DD-MM-YYYY. |
| **Document status** | | Draft · Submitted for verification · Verified · Approved · Superseded. |

03

# What is considered an incident for this system

**Type of incident:** Performance degradation · Erroneous output with impact · Discriminatory or biased output · Information leakage · Unauthorised action by an agent · Prompt injection or manipulation · Unavailability · Regulatory breach · Misuse of the system · Supplier incident.

| Type | Does it apply to this system? (Yes · No) | Specific example for this system | Planned detection (P25 alert or other route) |
|---|---|---|---|
| **Unauthorised action by an agent** ***(illustrative example)*** | Yes | The agent issues a refund above the limit | AL-02 |
| | | | |
| | | | |

04

# Severity

Common framework scale: **S1 Critical · S2 High · S3 Medium · S4 Low**. The full criteria are set out in document 37 and prevail over this guidance.

| Severity | Guidance | Example for this system |
|---|---|---|
| **S1 Critical** | Includes any possible serious incident under the EU AI Act and major incidents under DORA or NIS2 where applicable. | |
| **S2 High** | Relevant impact on people, customers, operations or compliance, contained or limited. | |
| **S3 Medium** | Limited impact, with no relevant effect on people or on reporting obligations. | |
| **S4 Low** | No appreciable impact; an anomaly that should be recorded. | |

05

# Roles during the incident

| Role | Holder | Deputy | Activated in | Responsibility |
|---|---|---|---|---|
| **Incident coordinator** | | | S1–S4 | Leads the response and decides on containment. Normally the AI Operations Owner. |
| **Technical lead** | | | S1–S3 | Diagnosis, technical containment and rollback. |
| **Information security** | | | Security and agent incidents | Attack analysis and preservation of evidence. |
| **Data protection** | | | If personal data are involved | Assess personal data breach and the rights of affected individuals. |
| **AI Risk Owner** | | | S1–S2 | Assess regulatory obligations and the effect on the risk register. |
| **Communication (Enterprise)** | | | S1–S2 | Coordinated internal and external messages. |
| **AI Sponsor** | | | S1–S2 | Business decisions and escalation to governing bodies. |
| **Incident recording** | | | S1–S4 | Timeline, decisions and evidence in P27. |

06

# Response phases

Internal target times are set by the company; they do not replace the regulatory time limits in document 37.

| Phase | What is done | Owner | Internal target time S1 | Internal target time S2 | Record |
|---|---|---|---|---|---|
| **Detection** | Receive alert or notification; open incident | On-call | | | P27 |
| **Classification** | Type and initial severity | Coordinator | | | P27 |
| **Containment** | Apply the actions in block 7 | Coordinator and technical lead | | | P27 |
| **Reporting check** | Review block 8 | Risk and data protection | | | P27 |
| **Resolution** | Correct the immediate cause | Technical lead | | | P27 |
| **Recovery** | Return to normal operation with authorisation | Coordinator | | | P27 |
| **Closure and lessons** | Root cause, corrective actions, lessons | Coordinator and risk | | | P27 · P12 |

07

# Prepared containment actions

| Action | When it is applied | Who can execute it | Procedure |
|---|---|---|---|
| **Kill switch** | Unauthorised action, injection with effect, leakage in progress | | P18 block 9 |
| **Reduce the autonomy level** | Degradation with risk of impact | | P19 |
| **Roll back to previous version** | Failure attributable to a recent change | | P19 |

| Action | When it is applied | Who can execute it | Procedure |
|---|---|---|---|
| **Disable an agent tool or permission** | Abuse of a specific tool | | P18 block 5 |
| **Revoke credentials** | Identity compromise | | P18 block 4 |
| **Withdraw or correct published content** | Erroneous or inappropriate content visible to third parties | | |
| **Preserve logs and evidence** | Always in S1 and S2 | | |

08

# Regulatory and contractual reports to be verified

Check boxes. For each incident, it is verified whether they apply; time limits are taken from document 37 and confirmed with legal counsel. This table does not assert time limits.

| ☐ | Report to be verified | Reference | Does it apply? (Yes · No · To be determined) | Who decides | Who reports | Time limit confirmed in document 37 and verification date | Evidence |
|---|---|---|---|---|---|---|---|
| ☐ | Serious incident involving a high-risk AI system | EU AI Act (obligations of the provider and of the deployer; document 34) | | | | | |
| ☐ | Information to the provider of the AI system | EU AI Act and contract (if the company is the deployer) | | | | | |
| ☐ | Personal data breach to the supervisory authority | GDPR, Article 33 | | | | | |
| ☐ | Communication to data subjects | GDPR, Article 34 | | | | | |
| ☐ | Major ICT-related incident | DORA | | | | | |

| ☐ | Report to be verified | Reference | Does it apply? (Yes · No · To be determined) | Who decides | Who reports | Time limit confirmed in document 37 and verification date | Evidence |
|---|---|---|---|---|---|---|---|
| ☐ | Significant incident | NIS2 and national transposition | | | | | |
| ☐ | Sector-specific reports | Company's sector regulation | | | | | |
| ☐ | Contractual obligations towards customers or suppliers | Contracts | | | | | |
| ☐ | Communication to affected individuals not required by law but appropriate **(Enterprise)** | Company policy | | | | | |

The report models, the reasoned decision not to report and the communications are in P51.

09

# Internal escalation

| Severity | Who is informed | Internal time limit | Reference |
|---|---|---|---|
| **S1** | AI Committee and board committee, in addition to the roles in block 5 | | Document 37 |
| **S2** | AI Committee and sponsor | | Document 37 |
| **S3** | AI Product Owner and AI Office | | Document 37 |
| **S4** | Record in P27 | | Document 37 |

If the incident reveals a breach of the framework (control disabled, unapproved change, gate skipped), a nonconformity with code NC-AAAA-NNN is also opened (P50, document 37).

10

# Drills

| Date | Scenario | Participants (roles) | Time to containment | Result (Passed · Passed with observations · Not passed) | Improvement actions |
|---|---|---|---|---|---|
| ***(illustrative example)*** | A document with hidden instructions causes an unauthorised external transmission | On-call, security, data protection, coordinator | 35 minutes | Passed with observations | Data protection had no reachable deputy; one is designated |

At Enterprise intensity, at least one drill should be carried out before G5 and repeated at the frequency set by the company.

11

# Quality criteria

Formal G5 and R6 criteria in document 21; incident process in document 37.

| # | Check | Status (Met · Not met · Not applicable · Pending) |
|---|---|---|
| **1** | The applicable incident types have a specific example and a detection route. | |
| **2** | Severity uses the S1–S4 scale and refers to the criteria in document 37. | |
| **3** | All roles have a holder and a deputy. | |
| **4** | Containment actions are prepared and linked to P18 and P19. | |
| **5** | Regulatory reports are identified as boxes to be verified, without unconfirmed time limits. | |
| **6** | Internal escalation reaches the AI Committee and the board committee in S1. | |

| # | Check | Status (Met · Not met · Not applicable · Pending) |
|---|---|---|
| 7 | At least one drill has been carried out (Enterprise). | |

12

## Approval and verification

| Function | Role | Name | Date | Signature or reference |
|---|---|---|---|---|
| **Author** | AI Operations Owner | | | |
| **Review** | Information security | | | |
| **Review** | Data protection | | | |
| **Clearance** | AI Risk Owner | | | |
| **Verifier** | AI Office (Lite) · AI Auditor (Enterprise) | | | |

Segregation of duties: the verifier is not part of the team that builds or operates the system.

13

## Version control

| Version | Date | Changes |
|---|---|---|
| **0.1** | 16-09-2026 | First version of the template. |

## External sources cited

Links to the official or primary source, checked before publication. Always verify the version in force on the date of use.

**Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)** · http

s://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng · Parlamento Europeo y Consejo de la UE · 14-12-2022

**Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)** · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng · Parlamento Europeo y Consejo de la UE · 27-04-2016

**Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA)** · https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng · Parlamento Europeo y Consejo de la UE · 14-12-2022

**Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)** · https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng · Parlamento Europeo y Consejo de la UE · 13-06-2024