| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | [Insert Registered Legal Entity Name Here] | | | | | | | |
| Document number:<br>P30 | | | | | Document Title:<br>**Incident Response Policy** | | | | | | | |
| Version:<br>1.0 | | Effective Date:<br>01.01.2025 | | | Document Owner: | | | | | | | |
| X | Policy | | Standard | | Procedure | | Form | | Register | | Other | |

| Revision history | | | | |
|---|---|---|---|---|
| **Revision number** | **Revision Date** | **Changes** | **Reviewed by** | **Process owner** |
| | | | | |
| | | | | |

| Approvals | | | |
|---|---|---|---|
| **Name** | **Title** | **Date** | **Signature** |
| | | | |
| | | | |

| Aligned with standards and regulations where applicable | | |
|---|---|---|
| **Standard/Regulation** | **Clause/Article** | **Comment** |
| ISO/IEC 27001:2022 | Clause 8.1, Clause 9.1 | |
| ISO/IEC 27002:2022 | Controls 5.25–5.27 | |
| NIST SP 800-53 Rev.5 | IR-1 through IR-9 | |
| EU GDPR | Article 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c) | |
| EU NIS2 | Article 23(1)–(4) | |
| EU DORA | Article 17(1)–(3) | |
| COBIT 2019 | DSS02, DSS04, MEA01 | |

PREVIEW ONLY

**Legal Notice (Copyright & Usage Restrictions)**

© 2025 Clarysec LLC. All rights reserved.

This document is the intellectual property of Clarysec LLC. No part may be copied, reused, redistributed, or modified for commercial or implementation purposes without explicit written permission.

Unauthorized use is strictly prohibited and may lead to legal action.

For licensing, contact: info@clarysec.com

<table>
<tr><td colspan="3"></td><td colspan="9">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="3">Document number:<br>P30</td><td colspan="9">Document Title:<br>Incident Response Policy</td></tr>
<tr><td colspan="2">Version:<br>1.0</td><td colspan="2">Effective Date:<br>01.01.2025</td><td colspan="9">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

1. **Purpose**
   1.1. This policy establishes a formal structure for the identification, reporting, analysis, containment, response, recovery, and post-incident evaluation of information security incidents affecting the organization.
   1.2. It ensures timely, coordinated, and effective responses to minimize operational disruption, financial loss, reputational damage, and regulatory non-compliance.
   1.3. The policy also facilitates continuous improvement of the organization's cyber resilience posture through lessons learned and integration of post-incident findings into governance, tooling, and training programs.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All personnel, including employees, contractors, consultants, and third-party service providers
      2.1.2. All information systems, applications, infrastructure, networks, and data—whether on-premises, in the cloud, or hybrid
      2.1.3. All types of security incidents, including but not limited to:
         2.1.3.1. Unauthorized access or privilege escalation
         2.1.3.2. Malware and ransomware attacks
         2.1.3.3. Denial-of-service (DoS/DDoS) attacks
         2.1.3.4. Data loss, leakage, or exfiltration
         2.1.3.5. Insider misuse or policy violations
         2.1.3.6. Physical security breaches impacting digital assets
   2.2. The policy encompasses detection, triage, investigation, escalation, containment, evidence handling, notification, recovery, and root cause analysis.
3. **Objectives**
   3.1. To establish a repeatable and scalable incident response capability that enables swift detection, classification, and mitigation of security incidents.
   3.2. To minimize the business impact of security events through structured containment, eradication, and system recovery procedures.
   3.3. To ensure incident reporting and response align with legal, regulatory, and contractual requirements—particularly those concerning breach notification timelines and evidence handling.
   3.4. To support transparency and accountability through proper logging, documentation, and metrics tracking for all security incidents.
   3.5. To promote continuous improvement through post-incident reviews, corrective actions, and stakeholder training.
4. **Roles and Responsibilities**
   4.1. **Chief Information Security Officer (CISO)**
      4.1.1. Owns the incident response framework, ensures policy enforcement, and oversees enterprise-wide incident coordination.

PREVIEW ONLY

4.1.2. Serves as the primary liaison with regulators, executive leadership, and external legal counsel during major incidents.

4.2. **Incident Response Coordinator**

[….]

**11. Reference Standards and Frameworks**

This policy aligns with global standards and regulatory frameworks that define structured, measurable, and auditable requirements for incident detection, response, notification, and recovery.

**ISO/IEC 27001:2022**

**Clause 8.1 – Operational Planning and Control**: Requires structured processes to manage risks, including incident response planning and execution.

**ISO/IEC 27002:2022 – Controls 5.25–5.27**

**Annex A Control 5.25 – Responsibilities for Information Security Incident Management**: Defines the need for designated roles and clear ownership in handling incidents.

**Annex A Control 5.26 – Information Security Incident Reporting**: Requires prompt internal reporting and communication of security events.

**Annex A Control 5.27 – Response to Information Security Incidents**: Enforces containment, eradication, and improvement processes post-incident.

Provides specific implementation guidance on defining responsibilities, workflows, notification obligations, and improvement mechanisms for incident handling.

**NIST SP 800-53 Rev.5**

**IR-1 through IR-9 – Incident Response Family**: Defines comprehensive requirements for planning, detection, analysis, containment, reporting, and post-incident remediation.

**AU-6 – Audit Review, Analysis, and Reporting**: Supports evidence collection and analysis as part of incident investigation.

**PL-2 – System Security and Privacy Planning**: Aligns incident response with organizational risk posture and contingency planning.

**EU GDPR (2016/679)**

This policy supports GDPR **Article 33** by defining internal reporting obligations and ensuring breach notification to supervisory authorities within 72 hours. It also aligns with **Article 34**, covering

PREVIEW ONLY

communication to affected data subjects and listing conditions under which notification is not required, per points **(2)(a)–(c)**.

**EU NIS2 Directive (2022/2555)**

**Article 23** mandates incident notification to national authorities within **24 hours**, followed by an intermediate update within **72 hours** and a final report within one month. This policy integrates these requirements and defines roles, escalation paths, and content obligations to comply with **Article 23(1)–(4).**

**EU DORA (2022/2554)**

**Article 17** requires financial entities to report major ICT-related incidents to their competent authority and the European Supervisory Authorities. This policy incorporates those requirements through defined classification, escalation, and breach notification workflows in alignment with **Article 17(1)–(3).**

**COBIT 2019**

**DSS02 – Manage Service Requests and Incidents**: Directs organizations to define, monitor, and optimize incident management processes.

**DSS04 – Manage Continuity**: Ensures response plans are aligned with business continuity and disaster recovery objectives.

**MEA01 – Monitor, Evaluate and Assess Performance and Conformance**: Supports post-incident evaluations and metrics-based improvements.

PREVIEW ONLY