					Insert Registered Legal Entity Name Here							
Document number: P31					Document Title: **Evidence Collection and Forensics Policy**							
Version: 1.0		Effective Date: 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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	
ISO/IEC 27002:2022	Controls 5.25–5.27, 8	
ISO/IEC 27035:2016	Parts 1 & 3	
NIST SP 800-53 Rev.5	IR-1 to IR-9, AU-6, PL-2	
NIST SP 800-101 Rev.1	Mobile Device Forensics	Mobile device forensics
NIST SP 800-86	Integrating Forensic Techniques	Integrating forensic techniques into incident response
EU GDPR	Articles 5, 33–34	
EU NIS2	Article 23(1)–(4)	
EU DORA	Article 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Purpose

1.1 This policy establishes a structured, legally defensible framework for the identification, collection, preservation, analysis, and disposal of digital evidence during actual or suspected security incidents.

1.2 It ensures that forensic readiness and evidence-handling processes:

1.2.1 Maintain evidentiary integrity and chain of custody

1.2.2 Support internal investigations, legal proceedings, and regulatory reporting

1.2.3 Align with internationally recognized forensic standards and legal admissibility criteria

1.3 This policy supports the organization's commitment to proactive incident response, legal compliance, and governance transparency while minimizing operational disruption.

2. Scope

2.1 This policy applies to:

2.1.1 All employees, contractors, vendors, and service providers engaged in system administration, incident handling, or investigative activities

2.1.2 All endpoints, servers, applications, networks, and cloud platforms under organizational control or contractual responsibility

2.1.3 Any incident or event requiring evidence handling, including:

2.1.3.1 Insider threats, data breaches, or fraud investigations

2.1.3.2 Misuse of systems or authentication credentials

2.1.3.3 Operational technology (OT) or industrial control incidents

2.1.3.4 Physical access violations involving digital assets

2.2 This policy also governs any engagement with third-party forensic service providers or law enforcement during legal or regulatory escalation, or in connection with regulatory proceedings.

3. Objectives

3.1 To enable rapid, secure, and policy-compliant evidence acquisition during security events or investigations.

3.2 To preserve the integrity, authenticity, and admissibility of collected digital evidence through strict access controls, logging, and verification procedures.

3.3 To ensure all forensic activities are coordinated with legal and regulatory obligations, including data protection, employment law, and international transfer restrictions.

3.4 To support post-incident analysis, root cause determination, and control improvement through high-quality forensic outputs.

3.5 To integrate forensic readiness into the overall Information Security Management System (ISMS), supporting audits, breach notifications, and executive decision-making.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures that all forensic operations are legally defensible, auditable, and risk-based.

4.1.2 Authorizes escalation to external legal authorities and forensic service providers.

4.2 Forensic Analysts / Incident Handlers

4.2.1 Lead the acquisition, preservation, and technical analysis of evidence.

4.2.2 Ensure chain of custody is properly documented and maintained.

4.2.3 Document all actions, findings, and tool configurations used during investigations.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 This policy shall be reviewed at least annually and updated as necessary to reflect:

9.1.1 Changes in laws, regulations, or case law affecting forensic procedures or data handling

9.1.2 Updates to industry-recognized forensic standards or toolsets

9.1.3 Lessons learned from post-incident reviews, legal disputes, or audit findings

9.1.4 Technological changes in the platforms, devices, or systems under investigation

9.2 The review process is owned by the CISO and shall include consultation with:

9.2.1 Legal and Compliance

9.2.2 Data Protection Officer (DPO)

9.2.3 Security Operations and Forensics teams

9.2.4 Internal Audit

9.3 All revisions shall be:

9.3.1 Version-controlled and stored in the policy repository

9.3.2 Communicated to affected stakeholders, including forensic and incident response teams

9.3.3 Accompanied by updates to relevant operating procedures and training materials

9.4 Interim reviews shall be triggered following any critical incident involving mishandling of evidence, failure in chain of custody, or legal admissibility issues.

10. Related Policies and Linkages

10.1 This policy is aligned with and supported by the following organizational policies:

10.1.1 P1 – Information Security Policy: Establishes the foundational mandate for investigations, evidence control, and compliance with applicable laws.

10.1.2 P5 – Change Management Policy: Ensures that systems under investigation are not altered during active forensic processes.

10.1.3 P14 – Data Retention Policy and Disposal Policy: Governs secure deletion and retention periods for evidence and case-related data.

10.1.4 P18 – Cryptographic Controls Policy: Defines encryption requirements for storing and transferring sensitive or evidentiary data.

10.1.5 P22 – Logging and Monitoring Policy: Ensures the availability of event logs and telemetry for evidence collection and forensic correlation.

10.1.6 P30 – Incident Response Policy: Defines incident triage and escalation paths that trigger forensic procedures.

10.1.7 P33 – Audit and Compliance Monitoring Policy: Validates adherence to forensic protocols and chain-of-custody requirements through regular audits.

11. Reference Standards and Frameworks

11.1 This policy is aligned with international forensic and incident-handling standards to ensure evidentiary integrity, legal defensibility, and cross-jurisdictional compliance.

11.2 ISO/IEC 27001

11.2.1 Clause 8.1 – Supports operational control of forensic readiness and evidence-handling procedures

11.3 ISO/IEC 27002

11.3.1 Annex A Control 5.25 – Responsibilities for Incident Management: Requires defined roles for handling information security incidents and investigations.

11.3.2 Annex A Control 5.26 – Reporting Information Security Events: Supports the collection of event-related artifacts as evidence.

11.3.3 Annex A Control 5.27 – Response to Information Security Incidents: Requires structured, evidence-based remediation and investigation.

11.3.4 Annex A Control 8.27 – Secure Development and Forensics (where applicable): Addresses the protection of systems and tools during investigations.

11.4 ISO/IEC 27035:2016 (Parts 1 & 3)

11.4.1 Outlines the principles of incident detection, response, and forensic readiness, including planning, chain of custody, and incident evidence management.

11.5 NIST SP 800-53 Rev.5

11.5.1 IR-1 to IR-9, AU-6, PL-2: Defines structured requirements for planning, detection, analysis, containment, and response to security incidents. Supports evidence collection and auditability under AU-6 and ensures alignment with system security and privacy plans under PL-2 during forensic investigations.

11.6 NIST SP 800-86

11.6.1 Provides guidance on integrating forensic processes into the broader incident response lifecycle and maintaining forensic readiness.

11.7 NIST SP 800-101 Rev.1

11.7.1 Focuses on best practices for acquiring, preserving, and analyzing digital media and mobile device evidence in a legally defensible manner.

11.8 EU GDPR (2016/679)

11.8.1 Article 5 – Principles relating to processing of personal data: Applies to evidence containing personal or sensitive data and requires minimization and purpose limitation.

11.8.2 Articles 33–34 – Data Breach Notification: Forensic data supports compliance with breach notification obligations and legal disclosure processes.

11.9 EU NIS2 Directive (2022/2555)

11.9.1 Article 23 – Reporting Obligations: Forensic documentation and findings support timely and accurate incident reporting to competent authorities.

11.10 EU DORA (2022/2554)

11.10.1 Article 17 – ICT Incident Reporting: Requires detailed root cause analysis and evidentiary records for major ICT-related incidents, particularly within the financial sector.

11.11 COBIT 2019

11.11.1 DSS01.07 – Manage Security Incidents: Requires incident documentation and investigative rigor.

11.11.2 DSS05.04 – Manage Security Investigations: Emphasizes the preservation of digital evidence and support for disciplinary and legal action.