					[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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 8.1	
ISO/IEC 27002:2022	A Controls 5.25–5.27, 8.27	
ISO/IEC 27035:2016	Parts 1 & 3	
NIST SP 800-53 Rev.5	R-1 to IR-9, AU-6, PL-2	
NIST SP 800-101 Rev.1		Mobile/Media Forensics
NIST SP 800-86		Integrating Forensic Techniques into Incident Response
EU GDPR	Article 5, 33–34	
EU NIS2	Article 23(1)–(4)	
EU DORA	Article 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05.04	

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, or regulatory reporting
      1.2.3. Align with internationally accepted forensic standards and legal admissibility criteria
   1.3. The 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 credentials
         2.1.3.3. Operational technology (OT) or industrial control incidents
         2.1.3.4. Physical access violations involving digital assets
   2.2. The policy also governs any interaction with third-party forensic services or law enforcement during legal escalations or regulatory proceedings.
3. **Objectives**
   3.1. To enable rapid, secure, and policy-aligned evidence acquisition during security events or investigations.
   3.2. To preserve the integrity, authenticity, and admissibility of collected digital evidence through strict control of access, logging, and verification procedures.
   3.3. To ensure all forensic activities are coordinated with legal and regulatory obligations, including data protection, labor law, and international transfer restrictions.
   3.4. To support post-incident analysis, root cause determination, and improvement of controls through high-quality forensic output.
   3.5. To integrate forensic readiness into the overall 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 entities 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 recorded and maintained.

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

4.3. **IT Administrators and System Owners**

[….]

11. Reference Standards and Frameworks

This policy is aligned with international forensic and incident handling standards, ensuring evidence integrity, legal defensibility, and cross-jurisdictional compliance.

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022

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

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

Annex A Control 5.27 – Response to Information Security Incidents: Enforces structured, evidence-driven remediation and investigation.

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

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

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

NIST SP 800-53 Rev.5

IR-1 to IR-9, AU-6, PL-2: Defines structured requirements for planning, detecting, analyzing, containing, and responding to security incidents. Supports the collection and auditability of evidence (AU-6) and ensures alignment with system security and privacy plans (PL-2) during forensic investigations.

NIST SP 800-86

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

NIST SP 800-101 Rev.1

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

EU GDPR (2016/679)

Article 5 – Principles relating to processing of personal data: Applies to evidence that contains personal or sensitive data, ensuring minimization and purpose limitation.

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

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

COBIT 2019

DSS01.07 – Manage Security Incidents: Mandates incident documentation and investigatory rigor.

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