					[Insert Registered Legal Entity Name Here]							
Document number: P31S					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	Clauses 6.1, 6.3, 8.1	
ISO/IEC 27002:2022	Controls 5.24–5.27	
ISO/IEC 27035-3:2016	Clause 6.3, 6.4, 7.3	
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU12, PE-18	
EU GDPR	Articles 33, 34	
EU NIS2	Articles 23	
EU DORA	Article 17(1), 17(2)	
COBIT 2019	DSS05.06, DSS05.07	

					[Insert Registered Legal Entity Name Here]										
Document number: P31S					Document Title: **Evidence Collection and Forensics Policy**										
Version: 1.0		Effective Date: 01.01.2025			Document Owner:										
X	Policy		Standard		Procedure		Form		Register		Other				

1. **Purpose**
   1.1. This policy defines how the organization handles digital evidence related to security incidents, data breaches, or internal investigations. It ensures that evidence is collected, stored, and preserved in a legally sound and audit-ready manner, supporting both internal decision-making and potential external actions.
   1.2. The policy enables small organizations to protect the integrity of logs, files, and system images while demonstrating due diligence under ISO/IEC 27001, GDPR, and related standards.
   1.3. It supports forensic readiness without requiring advanced technical resources or a full-time IT team by defining clear responsibilities, processes, and retention requirements.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All employees, IT providers, and external consultants involved in incident response, investigation, or breach analysis
      2.1.2. All company systems, including laptops, mobile devices, servers, email accounts, SaaS platforms, and cloud storage (e.g., Microsoft 365, Google Workspace)
      2.1.3. Any event requiring evidence for internal disciplinary action, legal defense, insurance claims, or regulator engagement
   2.2. This includes both real and suspected events involving:
      2.2.1. Data leakage
      2.2.2. Insider threat or misuse
      2.2.3. Security breaches (e.g., malware, unauthorized access)
      2.2.4. Customer complaints requiring digital validation
      2.2.5. Regulator or law enforcement inquiries
3. **Objectives**
   3.1. Ensure all evidence is collected and handled in a way that maintains its integrity, authenticity, and chain of custody.
   3.2. Prevent accidental modification, deletion, or mishandling of logs, files, or system images that may be needed for investigations.
   3.3. Provide a consistent, auditable approach to evidence management that meets legal and regulatory expectations (e.g., GDPR breach notification, NIS2 traceability).
   3.4. Define clear roles and responsibilities to ensure rapid, secure, and legally compliant evidence capture during security incidents.
   3.5. Support SME-level forensics readiness while minimizing complexity and avoiding disruption to day-to-day operations.
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Approves all formal investigations that require evidence collection.
      4.1.2. Reviews and signs off on incident reports involving potential legal or disciplinary actions.
      4.1.3. Decides whether external legal counsel or regulators must be notified.
      4.1.4. Ensures the policy is reviewed and updated regularly.

[….]

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 6.1 – Risk-based planning includes response readiness and evidence procedures.

Clause 6.3 – Supports improvement actions based on evidence from incidents.

Clause 8.1 – Requires operational controls for evidence integrity.

ISO/IEC 27002:2022

Controls 5.24–5.27 – Guide secure handling, post-incident reviews, and evidence-driven improvements.

ISO/IEC 27035-3:2016

Clauses 6.3, 6.4, and 7.3 to ensure proper planning, lawful collection, and secure handling of digital evidence during incident response, including preservation and chain-of-custody documentation.

NIST SP 800-53 Rev. 5

IR-07, IR-08, AU-09, and AU-12 ensures forensic readiness, audit log protection, and effective integration of evidence collection into the incident response lifecycle

NIST SP 800-86

Defines best practices for acquiring, analyzing, and protecting digital evidence during incident response.

EU GDPR

Article 33–34 – Require documentation and traceability of incidents and evidence when reporting personal data breaches.

EU NIS2 Directive (2022/2555)

Article 23 – Requires traceable incident reporting and secure evidence handling for essential and important entities.

EU DORA

Article 17(1) – Ensures that evidence related to ICT-related incidents is collected and stored in a way that supports forensic investigations.

Article 17(2) – Requires that financial entities retain all relevant data and logs associated with security events, aligned with forensic soundness and regulatory inquiries.

COBIT 2019

DSS05.06 – Monitor, detect, and report incidents: Emphasizes reliable logging for investigation support.

DSS05.07 – Investigate and act on incidents: Requires structured evidence handling to enable secure and auditable investigations.