					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**

Legal Notice (Copyright & Usage Restrictions)

(C) 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

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 6.1, 6.3, 8	Risk-based planning, improvement actions, and operational controls for evidence integrity
ISO/IEC 27002:2022	Controls 5.24–5.27	Guides secure handling, post-incident reviews, and evidence-driven improvements
ISO/IEC 27035-3:2016	Clauses 6.3, 6.4, 7	Ensures proper planning, lawful collection, and secure handling of digital evidence with chain-of-custody documentation
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Forensic readiness, audit log protection, and effective integration into incident response
EU GDPR	Articles 33, 34	Documentation and traceability for personal data breaches
EU NIS2	Article 23	Traceable incident reporting and secure evidence handling
EU DORA	Article 17(1), 17(2)	Ensures evidence collection, storage, and retention for ICT-related incidents, forensic soundness, and regulatory inquiries
COBIT 2019	DSS05.06, DSS05.07	Reliable logging and structured evidence handling for secure, auditable investigations

1. Purpose

1.1. This policy defines how the organization handles digital evidence related to security incidents, personal data breaches, or internal investigations. It ensures that evidence is collected, stored, and preserved in a legally defensible and audit-ready manner, supporting both internal decision-making and potential external action.

1.2. This 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, procedures, and retention requirements.

2. Scope

2.1. This policy applies to:

2.1.1. All employees, IT service 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 regulatory engagement

2.2. This includes both actual and suspected events involving:

2.2.1. Data leakage

2.2.2. Insider threats or misuse

2.2.3. Security incidents (e.g., malware, unauthorized access)

2.2.4. Customer complaints requiring digital validation

2.2.5. Regulatory or law enforcement inquiries

3. Objectives

3.1. Ensure all evidence is collected and handled in a manner that preserves its integrity, authenticity, and chain of custody.

3.2. Prevent accidental modification, deletion, or mishandling of logs, files, or system images that may be required 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 forensic 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 approves incident reports involving potential legal or disciplinary action.

4.1.3. Determines whether external legal counsel or regulators must be notified.

4.1.4. Ensures this policy is reviewed and updated regularly.

4.2. IT Support Provider / System Administrators

4.2.1. Collect and preserve digital evidence in accordance with secure procedures.

4.2.2. Document timestamps, system details, and handling steps.

4.2.3. Secure all collected materials in a protected location.

4.2.4. Assist with forensic analysis where required.

[... 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. Annual Policy Review

9.1.1. This policy must be reviewed at least once every 12 months by the General Manager (GM) to confirm:

9.1.1.1. Compliance with ISO/IEC 27001 Annex A controls

9.1.1.2. Continued relevance to current digital platforms and IT services

9.1.1.3. Adequacy of logging, evidence retention, and forensic readiness procedures

9.2. Trigger Events for Policy Revision

9.2.1. This policy must also be reviewed and updated after:

9.2.1.1. Any major incident requiring evidence collection

9.2.1.2. A failed audit or regulatory request where evidence integrity was questioned

9.2.1.3. Adoption of new tools or procedures for incident response or system monitoring

9.2.1.4. Legal or regulatory changes (e.g., updated GDPR or NIS2 guidance)

9.3. Change Approval and Distribution

9.3.1. All changes must be reviewed and approved by the GM.

9.3.2. The updated version must be shared with:

9.3.2.1. IT service providers and consultants involved in investigations

9.3.2.2. Any staff with system administration responsibilities

9.3.3. An updated copy must be retained in the company's policy archive and shared with auditors upon request.

10. Related Policies and Linkages

10.1. This policy is interdependent with the following SME-aligned policies:

10.1.1. P2S – Governance Roles and Responsibilities Policy: Establishes authority over incident investigations, evidence decisions, and legal/regulatory escalation.

10.1.2. P4S – Access Control Policy: Ensures only authorized personnel can access sensitive systems and logs during investigations.

10.1.3. P22S – Logging and Monitoring Policy: Provides the raw data used as forensic evidence and establishes retention, access control, and logging requirements.

10.1.4. P30S – Incident Response Policy: Triggers the need for evidence collection and defines the operational flow leading to forensic preservation.

10.1.5. P17S – Data Protection and Privacy Policy: Ensures any personal data collected as evidence is handled lawfully under GDPR and related regulations.

10.2. These policies work together to support legal defensibility, investigative integrity, and full ISO/IEC 27001:2022 audit readiness.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

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

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

11.1.3. Clause 8.1 – Requires operational controls for evidence integrity.

11.2. ISO/IEC 27002

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

11.3. ISO/IEC 27035-3

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

11.4. NIST SP 800-53 Rev. 5

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

11.5. NIST SP 800-86

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

11.6. EU GDPR

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

11.7. EU NIS2 Directive (2022/2555)

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

11.8. EU DORA

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

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

11.9. COBIT 2019

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

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