Digital Evidence Preservation Service Definition

Document title	Digital Evidence Preservation Service Definition		
Reference No.	IF-SER-018	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Adam Whitbread, Principal Digital Forensic Analyst		
Issue date	28/01/2026		

Digital Evidence Preservation Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Adam Whitbread	Review and comments	28/01/2026
1.0	Lisa Washer	Minor amendments and publish	28/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

Digital Evidence Preservation Service Definition

Contents

1. Digital Evidence Preservation Service

1.1 Service Overview

1.1.1 The Digital Evidence Preservation Service is delivered by IntaForensics, an accredited digital forensics provider operating under a UKAS-accredited ISO/IEC 17025 quality framework and certified to ISO/IEC 27001 for information security management. The service provides structured, defensible support to identify, secure, and preserve digital evidence following suspected or confirmed incidents, investigations, or legal matters.

1.1.2 Preservation activities are conducted by qualified digital forensic practitioners working in accordance with IntaForensics' accredited procedures and recognised forensic principles, ensuring evidential integrity, authenticity, and admissibility. The service supports subsequent forensic analysis, litigation, regulatory enquiries, and internal investigations by ensuring that digital evidence is preserved in a forensically sound and auditable manner.

1.1.3 IntaForensics' accredited delivery model, underpinned by ISO/IEC 17025 and ISO/IEC 27001 certification, provides assurance that evidence handling meets the expectations of courts, regulators, and other external stakeholders.

1.2 Service Objectives

1.2.1 The objectives of the Digital Evidence Preservation Service are to:

a) Preserve digital evidence in a forensically sound manner

b) Maintain evidential integrity and chain of custody

c) Prevent spoliation, alteration, or loss of relevant data

d) Support future forensic, legal, or regulatory processes

e) Provide defensible documentation and audit trails

2. Service Features

2.1.1 The Digital Evidence Preservation Service includes the following key features, delivered under IntaForensics' accredited operating model:

a) **UKAS-Accredited Forensic Delivery** – Evidence preservation conducted in accordance with ISO/IEC 17025-accredited forensic procedures**,** ensuring repeatability, integrity, and admissibility.

b) **Information Security Assurance** – All evidence handled within ISO/IEC 27001-certified information security management systems**,** including controlled access, secure storage, and audit logging.

c) **Forensically Sound Preservation** – Identification, acquisition, and preservation of digital evidence aligned to recognised forensic principles and best practice.

d) **Broad Evidence Coverage** – Support for devices, servers, removable media, cloud-based data, and log sources.

e) **Chain-of-Custody Management** – Comprehensive, auditable documentation of evidence handling from identification through preservation and handover.

f) **Court and Regulator Readiness** – Preservation outputs remember suitable for use in legal proceedings, regulatory enquiries, and audits.

3. Service Benefits

3.1.1 The Digital Evidence Preservation Service delivers the following benefits to organisations:

a) **Evidential Integrity and Admissibility** – Evidence preserved under ISO/IEC 17025-accredited processes**,** reducing the risk of challenge or exclusion.

b) **Regulatory and Legal Confidence** – Assurance that evidence handling meets the expectations of courts, regulators, and legal professionals.

c) **Reduced Risk of Data Loss or Contamination** – Structured, accredited preservation minimises spoliation and evidential compromise.

d) **Independent Specialist Assurance** – Preservation performed by accredited forensic practitioners independent of operational or IT teams.

e) **Secure and Compliant Handling** – Evidence protected throughout its lifecycle by ISO/IEC 27001-certified security controls**.**

f) **Strong Foundation for Investigations** – Preserved evidence is ready for subsequent forensic analysis, litigation, or regulatory review.

4. Scope of Service

4.1.1 The service is delivered in alignment with recognised digital forensic principles, including evidential integrity, repeatability, and transparency. Engagements may be coordinated through legal counsel to support legally privileged handling where required. Outputs are suitable for legal proceedings, regulatory enquiries, and audits.

4.2 In-scope activities

4.2.1 Delivered in accordance with IntaForensics' UKAS-accredited ISO/IEC 17025 laboratory framework and ISO/IEC 27001 information security management framework, the Digital Evidence Preservation Service includes the following activities. Where activities fall outside the scope of accreditation, this is explicitly identified and agreed during scoping.

a) Scoping and identification of potential digital evidence sources

b) Preservation planning and prioritisation based on volatility and risk

c) Forensic acquisition of digital devices, systems, and storage media

d) Logical and physical imaging where appropriate

e) Volatile data capture where feasible and authorised

f) Integrity verification using cryptographic hashing

g) Secure handling, transport, and storage of preserved evidence

h) Maintenance of full chain-of-custody and preservation records

i) Advisory support on evidence preservation strategy, scope, and limitations

4.3 Out-of-scope activities

4.3.1 Unless agreed separately, the following are out of scope:

a) Substantive forensic analysis or interpretation of evidence

b) Live remediation, system recovery, or rebuild activities

c) Provision of legal advice or representation

d) Continuous monitoring or managed evidence storage beyond agreed periods

4.4 Assumptions, Dependencies and Constraints

4.4.1 Delivery of the Digital Evidence Preservation Service is based on the following assumptions:

a) The client has lawful authority and a valid legal basis to identify, access, and preserve all in-scope digital evidence, including devices, systems, accounts, and data repositories.

b) Preservation activities are initiated promptly following identification of a potential incident or investigative requirement to minimise the risk of data alteration or loss.

c) Systems, devices, and data sources remain available for preservation and have not been materially altered prior to acquisition, except where required for safety, business continuity, or containment.

d) Relevant logging, audit trails, and data retention mechanisms were operational at the time of the incident or event.

e) The client will provide timely access to system owners, custodians, locations, and documentation required to support evidence identification and preservation.

f) Any legal privilege, confidentiality, or sensitivity requirements are identified and communicated at the outset or as they arise.

4.4.2 Service delivery is dependent on the following factors:

a) Availability and physical or logical access to in-scope devices, systems, cloud platforms, or storage media.

b) Timely cooperation from internal stakeholders, including IT, security, facilities, and management personnel.

c) Cooperation from third-party service providers or vendors where data is hosted externally or systems are managed by third parties.

d) Adequate system stability to support forensic acquisition without unacceptable operational risk.

e) Timely decision-making by client legal or investigative teams regarding scope, prioritisation, and handling requirements.

f) Availability of appropriate forensic tools, facilities, and specialist resources to meet urgency and technical requirements.

4.4.3 The following constraints may impact the scope, timelines, or completeness of preservation activities:

a) Volatile data may be lost if systems are powered down, restarted, or modified before preservation can occur.

b) Encryption, access controls, or proprietary technologies may restrict acquisition without credentials, keys, or vendor assistance.

c) Physical damage, device failure, or environmental factors may limit preservation options.

d) Preservation activities may be constrained by business continuity, safety, or operational requirements.

e) Forensic best practice prioritises evidential integrity and defensibility over speed, which may affect response timelines.

f) Findings and preserved evidence represent a point-in-time snapshot and may not capture subsequent or historical changes.

g) Service delivery is subject to specialist availability and agreed commercial terms.

5. Service Delivery Model

5.1 Engagement Model

5.1.1 The service is delivered on an ad-hoc consultancy basis and may be initiated in response to incidents, investigations, or legal matters. Scope, timelines, and deliverables are agreed at the outset.

5.1.2 The service may be delivered remotely, on-site, or through a hybrid approach, depending on evidence location, urgency, and technical requirements.

5.1.3 All preserved evidence is handled using secure storage, access controls, and confidentiality safeguards. Evidence is retained only for the agreed duration and purpose.

5.2 Delivery Phases

5.2.1 Delivery typically includes:

a) Evidence scoping and preservation planning

b) Identification and securing of evidence sources

c) Forensic acquisition and verification

d) Secure storage and documentation

e) Engagement closure and handover

5.3 Reporting and Deliverables

5.3.1 Deliverables may include:

a) Evidence preservation logs

b) Chain-of-custody documentation

c) Hash verification records

d) Preservation summary reports

Advisory notes on preserved evidence

6. Exit and Offboarding

6.1.1 Upon completion, preserved evidence is securely transferred, retained, or destroyed in accordance with agreed instructions and applicable legal obligations. Access is revoked and engagement closure confirmed.

7. Roles and Responsibilities

7.1 Service Provider Responsibilities

7.1.1 The service provider is responsible for delivering the Digital Evidence Preservation Service in accordance with agreed scope, recognised digital forensic principles, and applicable legal and regulatory requirements. This includes advising on evidence identification and preservation strategy, prioritising evidence sources based on volatility and risk, and executing forensically sound acquisition and preservation activities.

7.1.2 The service provider will identify and secure relevant devices, systems, storage media, and data sources, performing logical or physical acquisition as appropriate. Integrity of preserved evidence will be verified using hashing and validation techniques, with full chain-of-custody documentation maintained throughout. The provider is responsible for secure handling, transport, and storage of preserved evidence, ensuring access is controlled and auditable. The provider will document all actions, assumptions, limitations, and deviations from standard procedures, and will escalate risks or issues that may impact evidential integrity, timelines, or scope.

7.2 Client Responsibilities

7.2.1 The client is responsible for confirming lawful authority and legal basis to access, preserve, and retain digital evidence. This includes identifying relevant systems, devices, custodians, and locations; facilitating timely access to premises, infrastructure, and personnel; and ensuring internal stakeholders cooperate with preservation activities.

7.2.2 The client retains responsibility for determining investigation scope, legal strategy, and subsequent use of preserved evidence. The client is also responsible for decisions relating to system shutdowns, containment actions, or business continuity measures that may impact evidence preservation. Where required, the client will approve preservation plans and receive custody of preserved evidence following completion.

7.3 Legal Counsel Responsibilities (Where Applicable)

7.3.1 Where internal or external legal counsel is engaged, counsel is responsible for advising on legal privilege, evidential requirements, and disclosure obligations. Legal counsel may instruct or oversee preservation activities, approve preservation scope, and ensure that handling supports admissibility in legal or regulatory proceedings. Counsel may also coordinate legally privileged engagement and review preservation outputs.

7.4 IT, Security, and Operational Stakeholders (Where Applicable)

7.4.1 IT, security, and operational stakeholders are responsible for supporting safe and timely access to systems, devices, and environments. This includes providing system knowledge,

credentials where authorised, and guidance on operational risks. These stakeholders support preservation activities while balancing business continuity, safety, and security considerations.

7.5 Joint Responsibilities

7.5.1 The service provider and client share responsibility for effective communication, timely decision-making, and escalation of issues that may impact evidential integrity, operational impact, or legal obligations. All parties are responsible for maintaining confidentiality, supporting transparency and auditability, and ensuring that evidence preservation is conducted proportionately, defensibly, and in line with applicable legal and regulatory expectations.

*****END OF DOCUMENT*****