Forensic Data Wiping Service Definition

Document title	Forensic Data Wiping Service Definition		
Reference No.	IF-SER-023	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Adam Whitbread, Principal Digital Forensic Analyst		
Issue date	27/01/2026		

Forensic Data Wiping Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Adam Whitbread	Review and comments	26/01/2026
0.3	Lisa Washer	Amendments and comments	27/01/2026
0.4	Adam Whitbread	Review and comments	27/01/2026
1.0	Lisa Washer	Final amendments and publish	27/01/2026

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

Forensic Data Wiping Service Definition

Contents

1. Forensic Data Wiping Service

1.1 Service Overview

1.1.1 The Forensic Data Wiping 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 secure, verifiable, and irreversible erasure of data from digital devices and storage media in a manner that is auditable, defensible, and aligned to recognised forensic and information security standards.

1.1.2 The service ensures that data is permanently removed to prevent recovery, supporting device disposal, redeployment, decommissioning, and compliance with data protection, security, and governance obligations.

1.2 Service Objectives

1.2.1 The objectives of the Forensic Data Wiping Service are to:

a) Ensure irreversible destruction of data from digital media

b) Prevent unauthorised recovery of sensitive or regulated information

c) Support compliance with data protection and information security obligations

d) Provide verifiable and auditable evidence of data destruction

e) Deliver wiping activities in line with accredited forensic and security frameworks

2. Service Features

2.1.1 Key features of the Forensic Data Wiping Service include:

a) Information Security Assurance – Handling within ISO/IEC 27001-certified environments

b) **Forensically Verified Wiping** – Validation to demonstrate data is irrecoverable

c) **Media-Aware Methods** – Techniques matched to HDDs, SSDs, and flash media

d) **Audit-Ready Reporting** – Clear documentation and certificates of destruction

3. Service Benefits

3.1.1 The service delivers the following benefits:

a) Confidence that data is permanently and irreversibly destroyed

b) Reduced risk of data breaches arising from reused or disposed devices

c) Compliance with data protection, security, and governance requirements

d) Independent assurance of data wiping effectiveness using accredited and validated tools.

e) Defensible records suitable for audit, regulator, or legal review

4. Scope of Service

4.1.1 The service supports compliance with data protection legislation, information security standards, and organisational policies. All wiping activities are documented in a manner suitable for audit, regulatory enquiry, or legal scrutiny. Where required, engagement may be coordinated through legal or compliance teams.

4.2 In-scope activities

4.2.1 Delivered in accordance with recognised forensic and information security principles, and governed by IntaForensics' established quality and security management frameworks, the service includes:

a) Scoping and confirmation of wiping requirements and objectives

b) Identification and inventory of in-scope devices and storage media

Forensic data wiping of hard drives, SSDs, and removable media.

Use of approved wiping methods appropriate to media type

c) Verification of wipe effectiveness using forensic validation techniques

d) Secure handling, transport, and storage of devices prior to wiping

e) Documentation of wiping methods, results, and limitations

f) Issuance of data wiping certificates and reports

4.3 Out-of-scope activities

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

a) Physical destruction of media

b) Recovery or analysis of data prior to wiping

c) Provision of legal advice or regulatory interpretation

d) Ongoing asset disposal or lifecycle management services

4.4 Assumptions, Dependencies and Constraints

4.4.1 Service delivery assumes that:

a) The client has lawful authority and approval to irreversibly destroy data

b) Devices are not subject to legal hold, investigation, or preservation requirements

c) Devices are accessible and in a condition suitable for wiping

d) Wiping requirements and standards are clearly defined and agreed

4.4.2 Service delivery is dependent on:

a) Availability and timely access to in-scope devices and media

b) Cooperation from IT, security, and facilities teams

c) Stability and functionality of storage media

d) Timely client decisions regarding failed or incomplete wipes

4.4.3 The following constraints may apply:

a) Certain media types (e.g. damaged SSDs) may limit wipe effectiveness

b) Encryption or hardware-level protections may require alternative approaches

c) Forensic wiping prioritises verification over speed, impacting timelines

d) Findings represent a point-in-time validation of wipe effectiveness

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

5. Service Delivery Model

5.1.1 The Forensic Data Wiping Service is delivered using a controlled, repeatable delivery model designed to ensure security, verification, and auditability at every stage. All activities are performed by qualified IntaForensics practitioners operating in accordance with recognised forensic best practice and IntaForensics' established quality and information security management frameworks. Accredited or validated tools may be used, where appropriate, to support verification of data wiping effectiveness.

5.2 Engagement Model

5.2.1 The service is delivered on an ad-hoc or project basis. Scope, device volumes, wiping standards, timelines, and deliverables are agreed prior to commencement.

5.2.2 Wiping services may be delivered either at the client's premises using IntaForensics' mobile forensic kits or within IntaForensics' secure laboratory facilities, depending on device location, security requirements, and client preference. All wiping activities are conducted within controlled environments and governed by IntaForensics' information security management practices.

5.3 Engagement Initiation and Planning

5.3.1 Each engagement begins with formal initiation and planning to confirm scope, objectives, and constraints. This includes validation of lawful authority to wipe data, confirmation that devices are not subject to legal hold or evidential preservation requirements, and agreement of wiping standards, verification methods, reporting outputs, and timelines. Devices, media types, volumes, and delivery locations (on-site, remote, or hybrid) are confirmed at this stage.

5.4 Secure Device Intake and Control

5.4.1 In-scope devices are securely received, logged, and tracked using controlled inventory and asset management processes. Where devices are transported, secure handling and transfer procedures are applied. Access to devices is restricted to authorised personnel in accordance with ISO/IEC 27001 access control requirements**,** ensuring traceability and preventing unauthorised access.

5.5 Forensic Data Wiping Execution

5.5.1 Data wiping is performed using validated tools and approved methods appropriate to the specific storage technology (e.g. HDD, SSD, flash media). Wiping procedures are selected to ensure irreversible data removal and are executed in accordance with recognised forensic best practice, prioritising completeness and verifiability over speed. Accredited or

validated tools may be used, where appropriate, to support verification of data wiping effectiveness.

5.6 Verification and Validation

5.6.1 Following wiping, verification activities are undertaken to confirm the effectiveness of the wipe. This may include forensic validation techniques to demonstrate that data is no longer recoverable. Any failures or partial wipes are identified, documented, and addressed in line with agreed escalation procedures.

5.7 Documentation and Certification

5.7.1 All wiping and verification activities are fully documented to provide an auditable record of actions taken. This includes device inventories, wiping logs, validation results, and certificates of secure data wiping. Documentation is produced in a format suitable for audit, regulatory review, or contractual assurance.

5.8 Handover and Closure

5.8.1 Upon completion, devices are returned, redeployed, or disposed of in accordance with client instructions. Access to devices and data is revoked, and all engagement records are retained or destroyed in line with agreed retention requirements and IntaForensics' accredited procedures. Formal closure confirmation is provided.

6. Exit and Offboarding

6.1.1 Upon completion, wiped devices are returned, redeployed, or disposed of as instructed. All records are retained or destroyed in accordance with agreed retention requirements and IntaForensics' accredited procedures.

7. Roles and Responsibilities

7.1 IntaForensics Responsibilities (Service Provider)

7.1.1 IntaForensics is responsible for delivering the Forensic Data Wiping Service in accordance with the agreed scope and applicable legal and regulatory requirements, and in line with IntaForensics' established quality and information security management frameworks. Where appropriate, accredited or validated tools may be used to support verification of data wiping effectiveness.

7.1.2 Responsibilities include advising on appropriate wiping methods, securely handling and tracking devices, executing verified data wiping using validated tools and procedures, and performing post-wipe validation to confirm irrecoverability. IntaForensics will maintain full audit trails, produce accurate wiping documentation and certificates, and ensure all activities are performed in secure environments. Any limitations, failures, or deviations will be documented and escalated promptly.

7.2 Client Responsibilities

7.2.1 The client is responsible for confirming lawful authority to wipe data on in-scope devices and for identifying devices, media, and data sensitivity classifications. The client will ensure devices are released for wiping, free from legal hold or preservation requirements, and will provide timely access to locations, assets, and stakeholders.

7.2.2 The client retains responsibility for decisions relating to data retention, destruction approvals, asset disposal, and regulatory or contractual obligations arising from data wiping activities.

7.3 Joint Responsibilities

7.3.1 Both parties are responsible for effective communication, timely decision-making, and escalation of issues that may impact scope, timelines, or compliance. All parties must maintain confidentiality and ensure wiping activities are aligned to agreed objectives and legal obligations.

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