TUDUBLIN

Technology Services Guideline: Digital Forensics

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH

TU DUBLIN

TECHNOLOGICAL UNIVERSITY DUBLIN

1. Introduction

In today's interconnected world, digital information plays a critical role in academic, operational, and administrative processes at TU Dublin. With the reliance on digital systems, the potential risks of unauthorized access, cyber threats, and policy violations have also increased. Digital forensics is essential to effectively investigate and mitigate these risks, ensuring that any digital evidence related to security incidents, breaches, or misconduct is handled in a lawful, ethical, and structured manner.

The primary purpose of this Digital Forensics Guideline is to provide guidance for conducting digital forensic investigations at TU Dublin.

This **Digital Forensics Guideline** aligns with the following cyber security framework and controls:

National Institute of Standards and Technology Cybersecurity Framework 2.0

- Incident Analysis (RS.AN)
    - RS.AN-03
    - RS.AN-06
    - RS.AN-07

2. Definitions

Digital Forensics: The process of identifying, collecting, preserving, analysing, and documenting digital evidence in a manner that maintains its integrity and ensures it can be used in investigations, legal proceedings, or to support policy enforcement.

Digital Evidence: Any information stored or transmitted in digital form that may be relevant to an investigation. This includes data from computers, mobile devices, network systems, storage media, and cloud services.

Chain of Custody: A documented process that tracks the handling and movement of digital evidence from the point of collection to its presentation in an investigation. This documentation is essential for ensuring evidence integrity and admissibility in legal proceedings.

Incident: Any event or action that threatens the confidentiality, integrity, or availability of TU Dublin's digital systems, data, or assets, including suspected cybersecurity breaches, policy violations, or other forms of unauthorized activity.

Incident Response: A structured approach to addressing and managing security incidents to minimize impact and support recovery. Incident response includes initial detection, assessment, containment, and investigation phases.

Preservation of Evidence: Actions taken to protect digital evidence from alteration, deletion, or unauthorized access, ensuring its integrity is maintained throughout the investigative process.

3. Digital Forensics Guidelines

This section outlines the key principles, processes, and standards for conducting digital forensics at TU Dublin.

If an official Digital Forensic investigation is required by TU Dublin a fully qualified Cyber Security Third Party will be engaged to conduct an independent and thorough investigation. However, not all digital investigations within the University require this level of independent analysis. Digital investigation may be required to be completed by internal TU Dublin staff for many reasons including minor data breach investigations, freedom of information requests, cyber incident analysis, etc. The guidelines below are intended to provide internal staff with guidance on best practice for handling digital evidence and managing investigations in an ethical, and consistent manner.

1. Roles and Responsibilities

- **Designated Investigation Personnel**: While a dedicated forensics team is not in place, specific roles within TS, data security, and legal or compliance staff may be required to handle some digital forensic responsibilities. These individuals may be responsible for the collection, preservation, and preliminary analysis of digital evidence.
- **University Leadership**: University leadership authorizes investigations and oversees the allocation of resources. Leadership ensures investigations are warranted and compliant with institutional standards.
- **Legal and Compliance Advisors**: Advisors within the legal and compliance departments may provide guidance on the legal and regulatory aspects of digital investigations, ensuring that all activities adhere to data protection laws, privacy regulations, and ethical standards.
- **Data and System Custodians**: Staff who manage or oversee access to university systems and data should support digital investigations by facilitating access to relevant digital assets, while ensuring data security and integrity during forensic processes.

2. Digital Evidence Handling

- **Evidence Preservation**: Digital evidence should be preserved in a way that maintains its original state. Proper handling protocols, such as logging all access and preventing unauthorized modifications, are essential to maintaining evidence integrity.
- **Chain of Custody**: A documented chain of custody should be maintained for all digital evidence, recording each access, transfer, and any relevant actions taken. This record ensures accountability and supports the admissibility of the evidence.
- **Integrity Verification**: Basic techniques, such as hashing, may be used to verify that digital evidence remains unchanged throughout the investigation process.
- **Access Control and Confidentiality**: Access to digital evidence is restricted to authorized personnel only, ensuring confidentiality and preventing unauthorized exposure of sensitive information.

3. Investigation Procedures

- **Initiation of Investigation**: Investigations should be initiated following a report or detection of a security incident, policy violation, or suspected unapproved activity. Authorization from management is required before proceeding.

- **Identification and Collection of Evidence**: Evidence collection should focus on gathering only the necessary data to investigate the specific incident. Tools and techniques used should ensure that evidence remains untampered and is collected in a manner that can support future proceedings.
- **Basic Analysis and Documentation**: Designated personnel should conduct an initial analysis to understand the nature and scope of the incident. Each action taken should be documented thoroughly, ensuring that the process is transparent and can be reviewed if needed.
- **Reporting Findings**: After the investigation, a summary report should be prepared, outlining the findings, methods used, and any recommended actions. This report should be reviewed by management, as appropriate.

4. Incident Response and Escalation

- **Initial Response**: An incident response plan is followed to assess the situation and determine whether further forensic investigation is needed. This initial response may involve containing the incident, securing affected systems, and preserving data.
- **Escalation Protocols**: Should evidence indicate serious policy violations, criminal activity, or significant security risks, the investigation will be escalated to university leadership. This may involve coordination with external cybersecurity specialists or law enforcement.
- **Remediation and Recommendations**: Following an investigation, recommendations for improving security practices and preventing similar incidents in the future should be documented. These suggestions aim to strengthen TU Dublin's overall cybersecurity posture.

5. Compliance and Legal Considerations

- **Data Protection and Privacy**: All digital forensic activities are conducted in accordance with data protection and privacy laws, such as GDPR, to ensure that individual rights are respected throughout the investigative process.
- **Legal and Regulatory Compliance**: TU Dublin's digital forensics activities should align with applicable laws and industry best practices, ensuring that the university adheres to both educational and cybersecurity standards.
- **Confidentiality and Ethical Standards**: TU Dublin is committed to confidentiality and ethical standards in all forensic investigations. Strict access controls are implemented to protect sensitive information, and confidentiality agreements may be used where appropriate.
- **Incident Reporting to Authorities**: If required by law or in situations of public safety, TU Dublin will report relevant findings to regulatory or legal authorities. Such decisions will be made in consultation with university leadership.

6. Training and Awareness

- **Basic Forensics Training**: Staff involved in digital forensics should receive foundational training in evidence handling, legal obligations, and TU Dublin's forensic protocols.
- **Awareness and Incident Reporting**: TU Dublin will promote awareness of cybersecurity policies, including the importance of incident reporting. Faculty, staff, and students are encouraged to report suspicious activities and potential security incidents as soon as possible.

4. Summary

This document outlines TU Dublin's digital forensic protocols, including escalation procedures for serious violations, remediation recommendations, compliance with legal standards such as GDPR, and adherence to ethical confidentiality. It emphasizes the importance of cybersecurity training and awareness, promoting incident reporting among faculty, staff, and students. The document also details the responsibilities for evidence handling and the mandatory reporting to authorities when necessary.

Appendix 1: Cyber Chain of Custody Form

Evidence Details

Field	Details
Evidence Description	[User to fill in]
Collection Date	[User to fill in]
Individual Responsible for Handling the Evidence	[User to fill in]
User Number	[User to fill in]
Reason Obtained	[User to fill in]
Incident Number	[User to fill in]
Evidence Type / Manufacturer	[User to fill in]
Model Number	[User to fill in]
Serial Number	[User to fill in]
Content Owner / Title	[User to fill in]
Content Description	[User to fill in]
Content Owner Contact Information	[User to fill in]
Forensic Agent	[User to fill in]
Creation Method	[User to fill in]
HASH Value	[User to fill in]
Creation Date/Time	[User to fill in]
Forensic Agent Contact Information	[User to fill in]

Chain of Custody

Tracking Number	Date/Time	Released By	Received By	Reason for Change
[User to fill in]	[User to fill in]	[User to fill in]	[User to fill in]	[User to fill in]
[User to fill in]	Date:	Name/Title	Name/Title	[User to fill in]
[User to fill in]	Time:	Signature	Signature	[User to fill in]
[User to fill in]	Date:	Name/Title	Name/Title	[User to fill in]
[User to fill in]	Time:	Signature	Signature	[User to fill in]
[User to fill in]	Date:	Name/Title	Name/Title	[User to fill in]

Document Control Summary

Area	Document Information
Author	Information Security Governance, Risk & Compliance
Status	Approved
Approved by	David Robinson – Chief Information Officer
Approval date	25th April 2025
Document Classification	TU Dublin Public