

[Organization Logo, Name, and Details]

Digital Forensics Readiness Policy Document

[Date]

Document Control

Organization	[Council Name]
Title	[Document Title]
Author	[Document Author – Named Person]
Filename	[Saved Filename]
Owner	[Document Owner – Job Role]
Subject	[Document Subject – e.g., IT Policy]
Protective Marking	[Marking Classification]
Review Date	

Revision History

Revision Date	Revisor	Previous Version	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

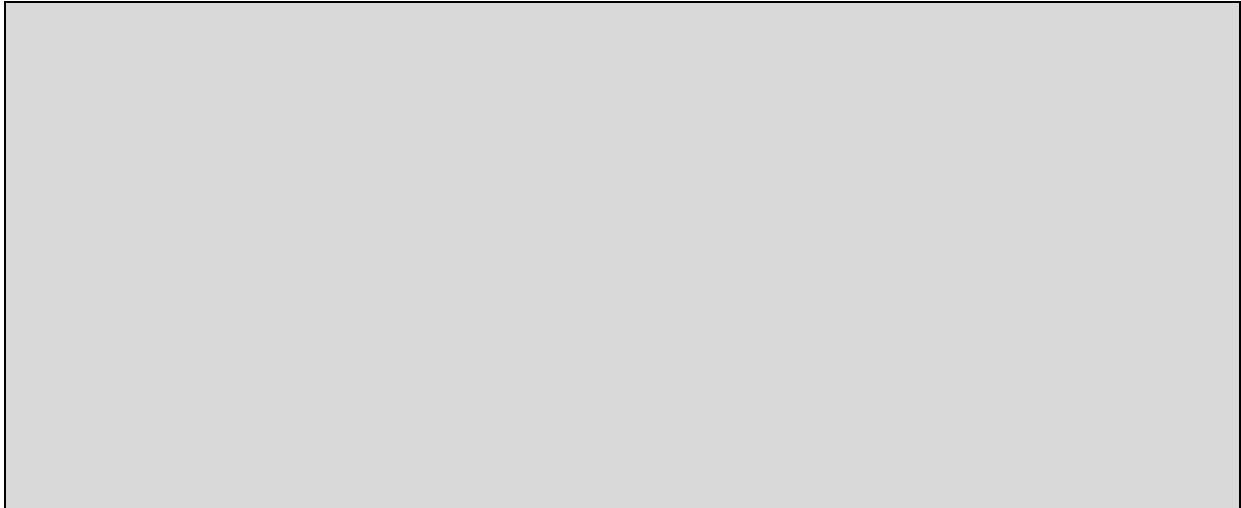
Contributors

Organizations involved in the development of this policy:

Organization Name	Contact Address	Contact Number

1. Policy Statement

[This policy has been developed to define the scope of digital forensic readiness <Organization Name> and to elucidate the <Organization Name's> assurance toward increasing the potential to use digital information, in particular for post-incident response and investigation of major security incidents.]



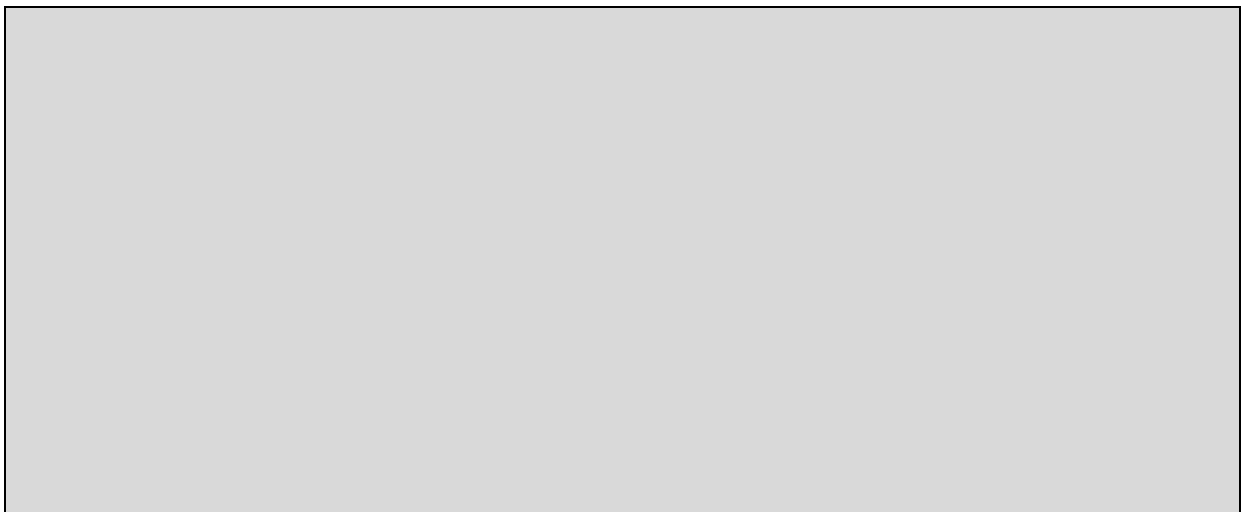
2. Objective

*[*Forensic policy is a set of procedures describing the actions an organization must take to preserve and extract forensic evidence during an incident. Organizations must create a forensics policy and implement it for the incident responders to follow.*

**Define purpose of creating forensic readiness policy.*

**Define goals for digital forensic planning.*

**Define forensic readiness principles.]*



3. Definition

*[*Forensic Readiness: Forensic readiness refers to an organization's ability to make optimal use of digital evidence in a limited period of time and with minimal investigation costs.*

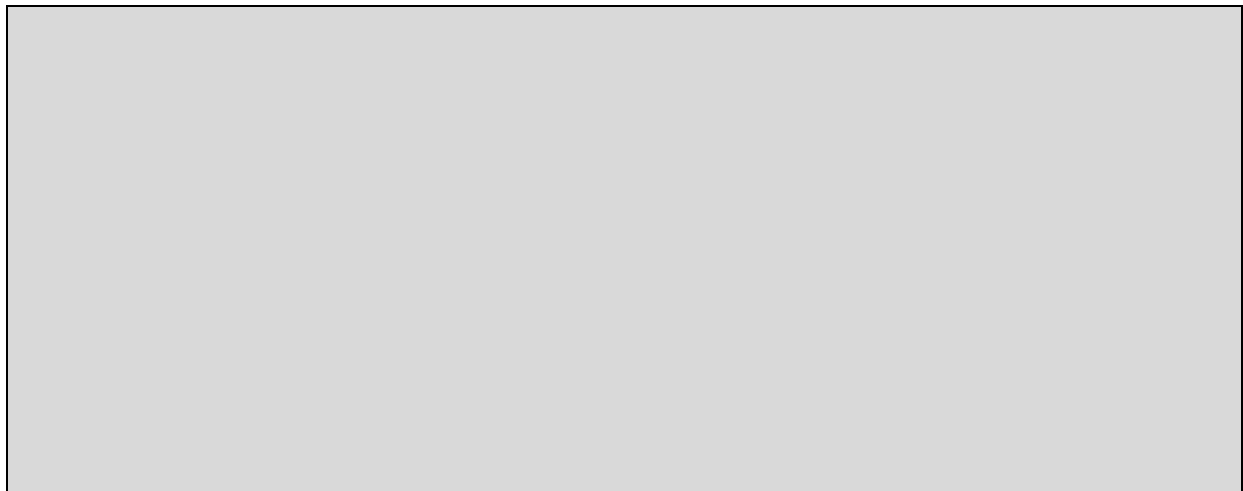
Forensic Readiness Planning: Forensic readiness planning refers to a set of processes required to achieve and maintain forensics readiness. It is the process of building a structure that enables an organization to deal with legal procedures, following a criminal offense. This structure equips the organization to properly deal with incidents and evidence, while covering every aspect of the criminal procedure.

Digital Evidence: Digital evidence is defined as "any information of probative value that is either stored or transmitted in a digital form" and helps incident responder/investigator find the perpetrator.]



4. Procedure/Implementation

[Describe key activities involved in the implementation of forensic readiness program and these activities must be incorporated into the forensic readiness plan.]



5. Forensic Readiness Plan

[A forensic readiness plan must be developed to support potential digital forensic investigation. This plan must be regularly tested and evaluated at least once per annum.]

The plan should cover the following:

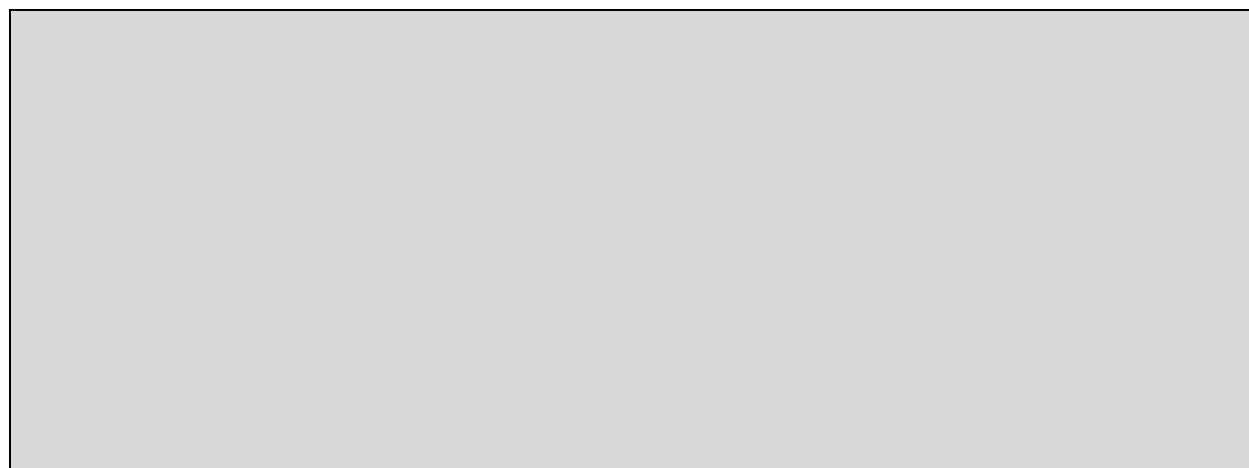
Ownership	
Capabilities	
Resources Equipment	
Task Flow	[Include single point of contact, relationship to incident management team, digital evidence process, classification of investigation, first response actions, securing the scene, recovery of data, collection of evidence, analysis, and recording of actions taken.]
Reporting on Investigation	
Case Review	

6. Policy Scope

[Example:

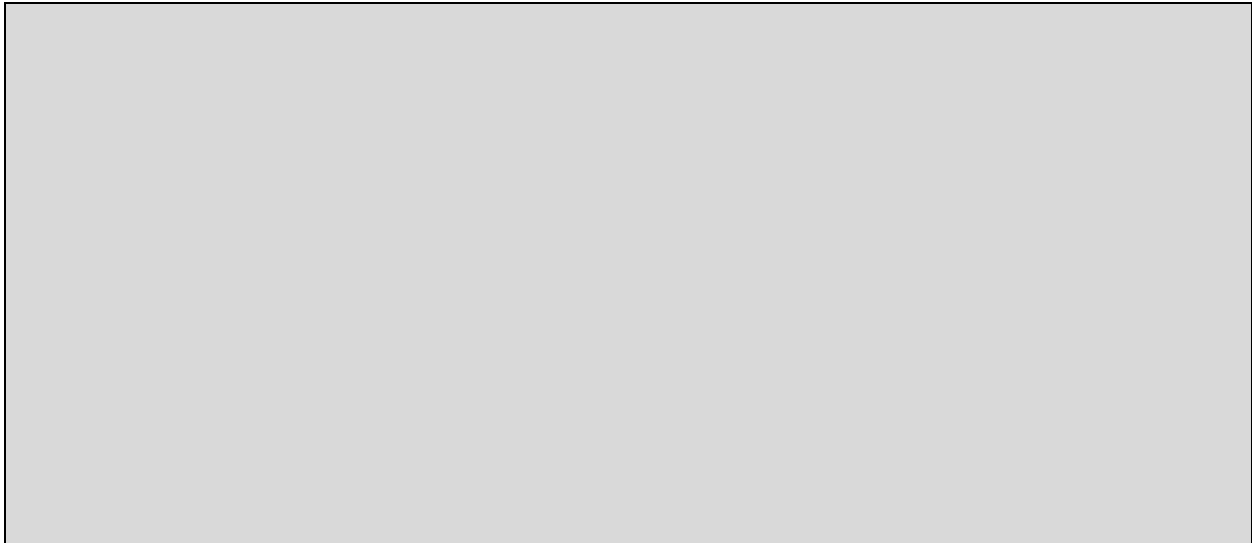
**This document is applicable to all Departments, Committees, Employees of the organization, Partners, third-parties and agents, etc. who use the <Organization Name> IT services and equipment or have access to customer information or <Organization Name> information.*

**An agreement must be made between the two parties regarding acquisition and storage of digital evidence particularly when the investigation is outsourced.]*



7. Applicability

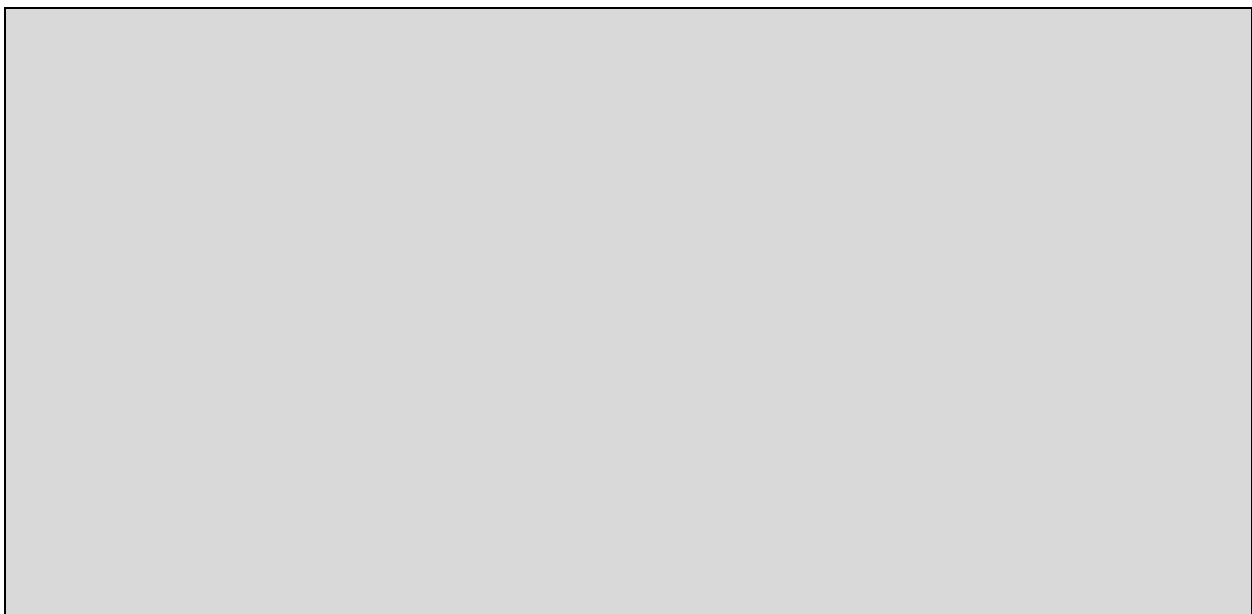
[List out all the departments/partners/employees for whom this policy is applicable.]*



8. Policy Compliance

[If any user is found to have violated this policy, they may be subject to [Organization Name's] disciplinary procedure. If a criminal crime is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).]*

** If you need any further clarifications in understanding the implications of this policy or how it is applicable to you, seek assistance from <Concerned Department Name>.]*



9. Communication

*[*List out all the departments and staff to whom this policy is applicable.*

**This policy must be made available to all the departments and staff listed below.]*

--

10. Policy Governance

[Table given below identifies who within the <Organization Name> is accountable, responsible, informed, or consulted regarding to this policy. Policy governance definitions include:

** Responsible: Personnel responsible for developing and executing this policy*

** Accountable: Personnel having ultimate accountability and authority for this policy*

** Consulted: Personnel or groups to be consulted before the final implementation or amendment of this policy*

** Informed: Personnel or groups to be informed post policy implementation or amendment.]*

Responsible:	[Insert appropriate Job Title – e.g., Head of IT Services, Head of HR Department, etc.]
Accountable:	[Insert appropriate Job Title – e.g., Director of Finance, etc. * Note: Only one role is held accountable.]
Consulted:	[Insert appropriate Job Title, Department or Group – e.g., Policy Department, Employee Groups, etc.]
Informed:	[Insert appropriate Job Title, Department or Group – e.g., All Employees of the Organization, All Part-Time Staff, All Contract-based Staff, etc.]

11. Legislation

*[*For the implementation of this policy the legislation given below may be referred.*

**Example: Data Protection Act, Human Rights Act, Computer Misuse Act, etc.]*

--

12. Review and Revision

[This policy will be reviewed whenever deemed appropriate but no less frequently than every <Specify months/years>.

Policy review will be undertaken by <Name of the Reviewer, Job Title, and Department>.]

Review Period:	
Review Date:	
Name of the Reviewer:	
Job Title:	
Department:	

13. References

[List out all the <Organization Name's> policy documents that are directly relevant to this policy. Example: Information Governance Policy, Acceptable Usage Policy, Information Protection Policy, Intellectual Property Policy, etc.]

Policy Number	Policy Name