

**[Organization Logo, Name, and Details]**

# **Incident Handling and Response Policy and Procedure Document**

**[Date]**

## Document Control

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

## Revision History

<b>Revision Date</b>	<b>Revisor</b>	<b>Previous Version</b>	<b>Description of Revision</b>

## Document Approvals

This document requires the following approvals:

<b>Sponsor Approval</b>	<b>Name</b>	<b>Date</b>

## Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

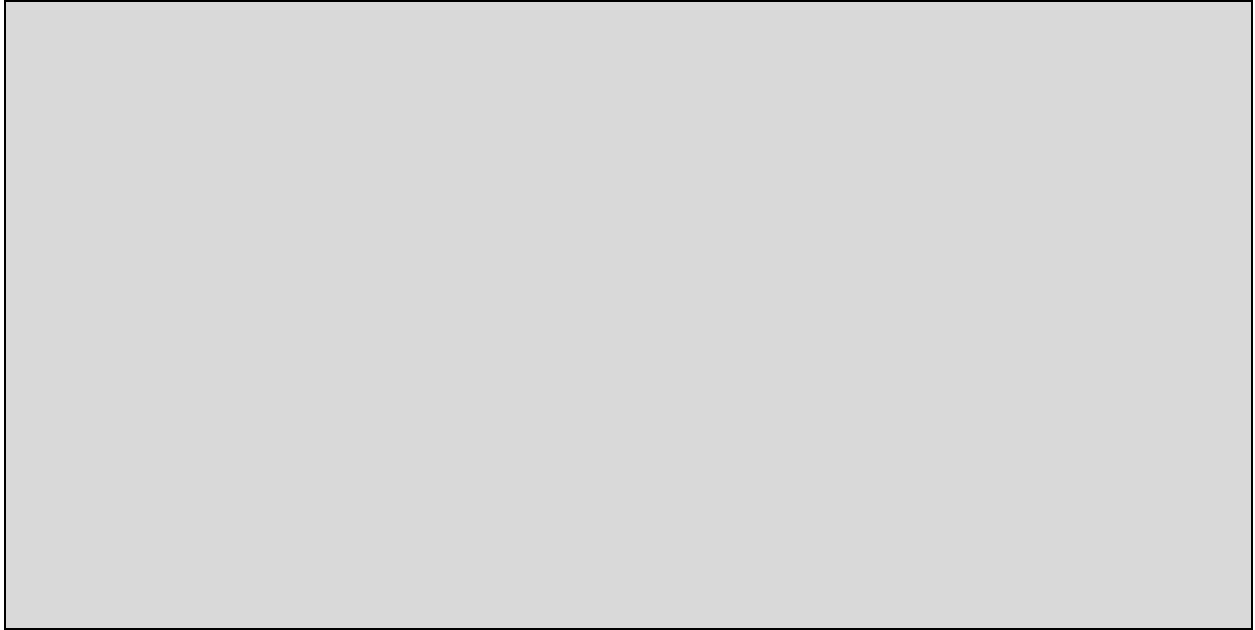
## Contributors

Organizations involved in the development of this policy:

Organization Name	Contact Address	Contact Number

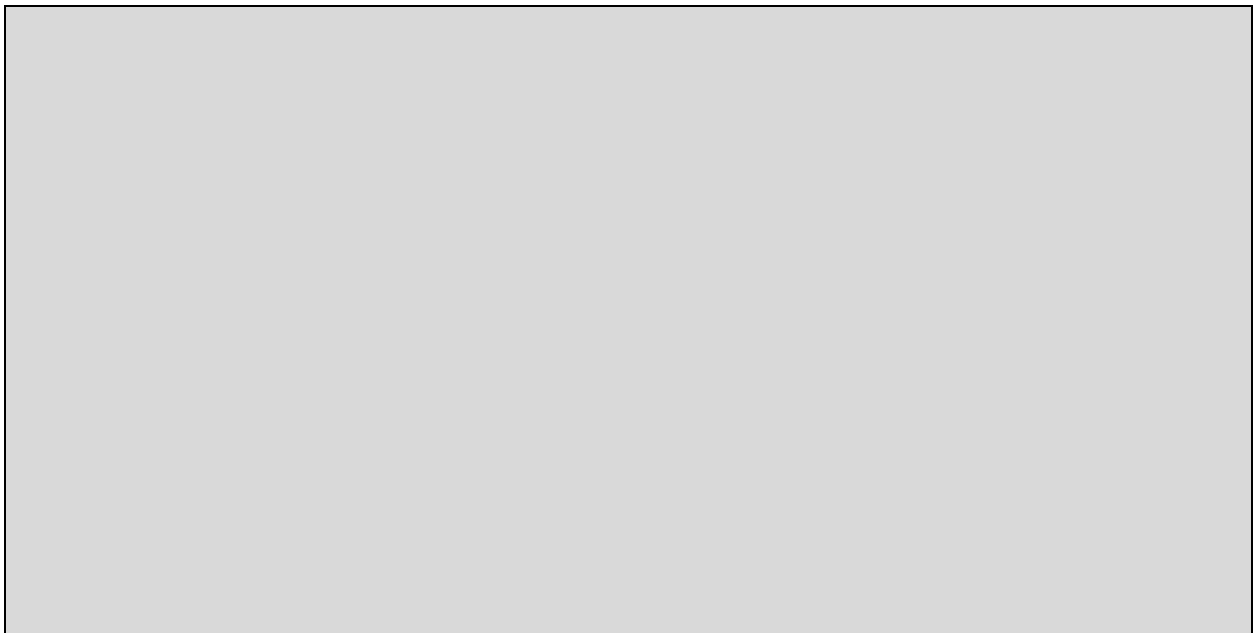
## 1. Policy Statement

*[<Organization Name> will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody of the organization.]*

A large, empty rectangular box with a thin black border, intended for additional content or a diagram related to the Policy Statement.

## 2. Purpose

*[The objective of this policy is to ensure that [Organization Name] reacts appropriately to any actual or suspected security incidents relating to information systems and data.]*

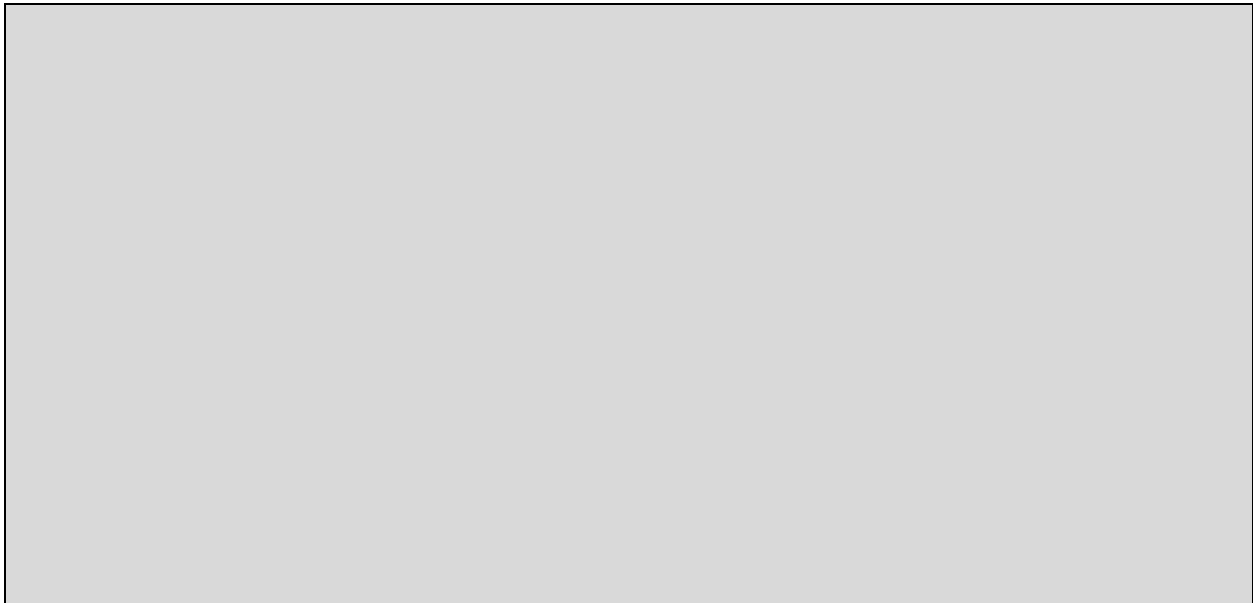
A large, empty rectangular box with a thin black border, intended for additional content or a diagram related to the Purpose section.

### 3. Scope

*[\*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.*

*\*All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the organization's systems and information.*

*\*All users are responsible for the safe and secure use of technology and the information that it holds.]*



### 4. Definition

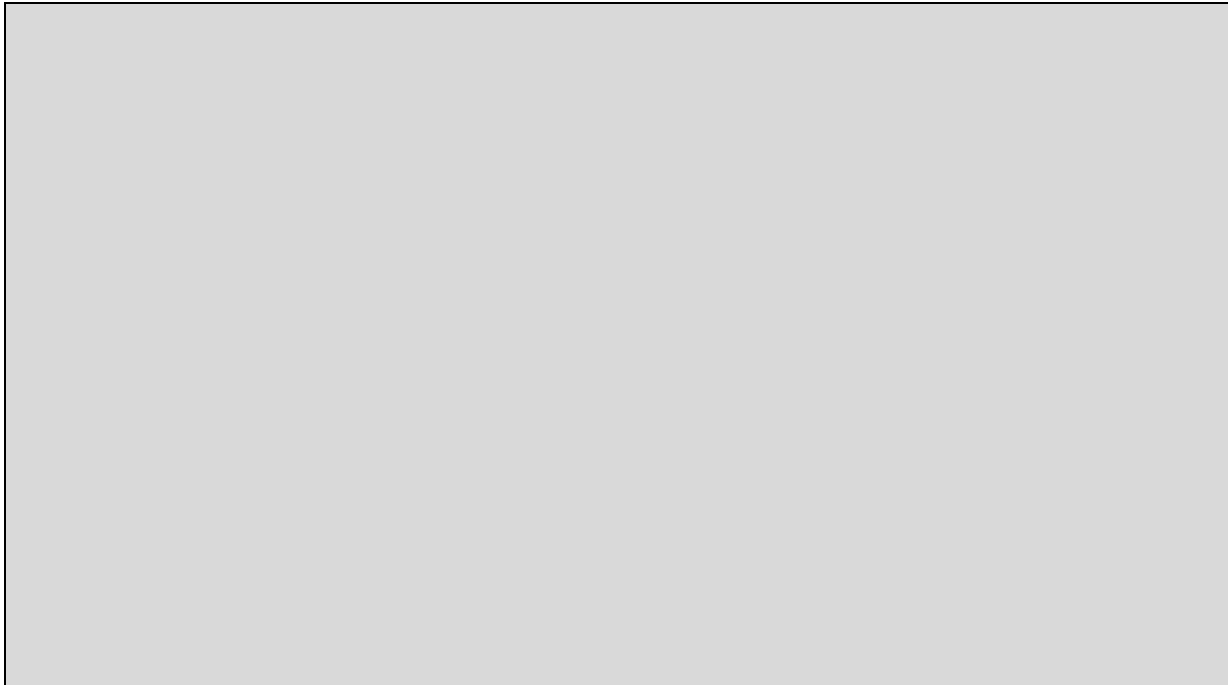
*[\*This policy must to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse activity which is likely to lead to a security incident.*

*\*Information security incident is a network or host activity that potentially threatens the security of information stored on network devices and systems with respect to confidentiality, integrity, and availability. It might be any real or suspected adverse event in relation to the security of computer systems or networks.*

*\*Some of the information security incidents include:*

- *Malicious Code or Insider Threat Attacks*
- *Unauthorized Access*
- *Unauthorized Usage of Services*
- *Email based Abuse*
- *Espionage*

- *Fraud and Theft*
- *Employee Sabotage and Abuse*
- *Network and Resource Abuses*
- *Resource Misconfiguration Abuses.]*



## 5. Risks

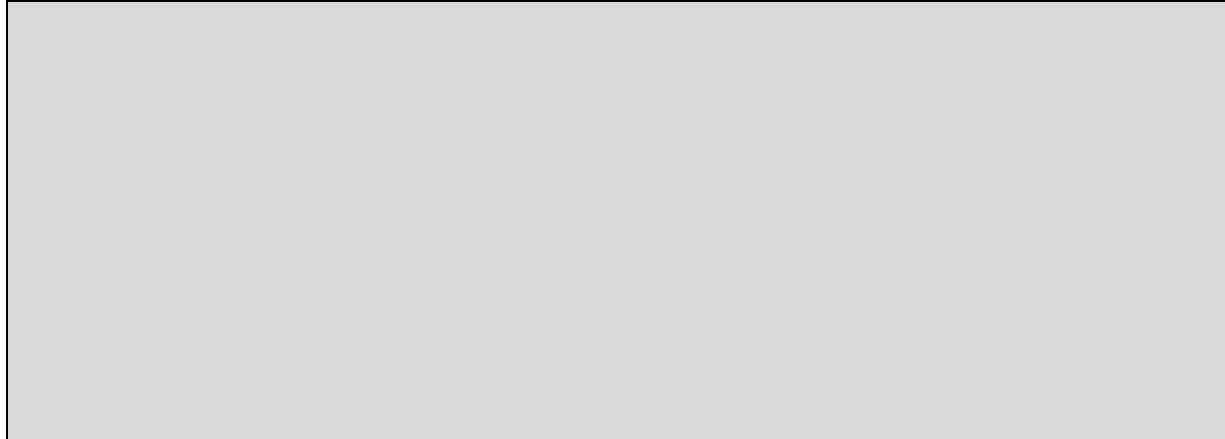
*[<Organization Name> recognizes that there are risks associated with users or processes accessing and handling information in order to perform various organizational business activities.]*

*This policy aims in mitigating the listed below risks:*

<b>Risk Description</b>	<b>Type of Impact (Low/Medium/High)</b>	<b>Recommendation(s)</b>

## 6. Procedure for Incident Handling and Response

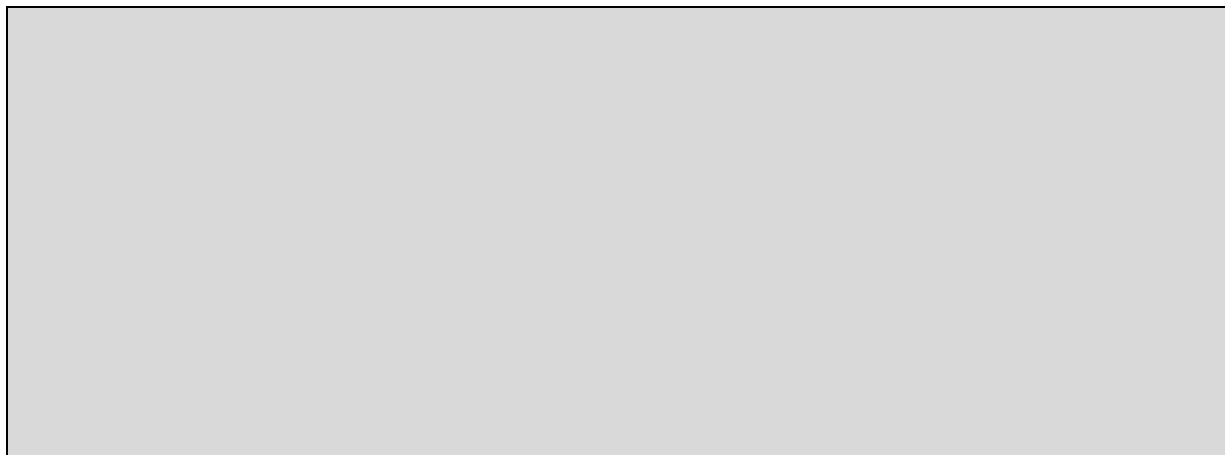
*[Events and malicious activities need to be reported at the earliest possible stage as they need to be assessed by an [Name of the Personnel – e.g., Information Security Officer/Advisor]. The Officer [or other named role] enables the [Name of the department – e.g., Incident Handling and Response Team] to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the [Name of the department – e.g., Incident Handling and Response Team] to gain as much information as possible from the business users to identify if an incident is occurring or has occurred.]*



## 7. 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>.]*



## 8. Policy Governance

*[The 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.]*

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

## 9. 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>.]*

<b>Review Period:</b>	
<b>Review Date:</b>	
<b>Name of the Reviewer:</b>	
<b>Job Title:</b>	
<b>Department:</b>	



## 10. References

*[List out all the <Organization Name's> policy documents that are directly relevant to this policy.  
Example: Email Policy, IT Access Policy, Internet Usage Policy, Information Protection Policy, etc.]*

Policy Number	Policy Name

## 11. Key Points to be Noted

*[List out all the important instructions to be followed by all the members of the organization related to this policy.]*

*Example:*

*\* All the staff should report any suspected or real incidents immediately by <include appropriate details here>*

*\* <Organization Name> maintains your anonymity when reporting a security incident*

*\* If you are unsure with any points in this policy, you can consult <Concerned Department or Authorized Person Name>.]*

Sr. No.	Instructions