**Insert Here Logo**

**Incident Management Policy**

**CONFIDENTIAL INFORMATION**

This document is the property of ABC Organization: it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the document owner. Dissemination, distribution, copying, or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of ABC Organization **Copyright © 2022**

**Table of Contents**

[Document Revision History 3](#_Toc97219601)

[Incident Management Policy 4](#_Toc97219602)

[1.1 Introduction 4](#_Toc97219603)

[1.2 Purpose 4](#_Toc97219604)

[1.3 Scope 4](#_Toc97219605)

[1.4 Incident Management Policy for ABC Organization 4](#_Toc97219606)

# Document Revision History

|  |  |
| --- | --- |
| **Author(s)** |   |
| **Status** | Version 1.0 |
| **Distribution** |  |
| **Reviewers** | **Date** | **Version** | **Description** | **Comments** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Incident Management Policy

## Introduction

Incident Management policy shall enable the response to a major incident or disaster by implementing a plan to restore the critical business functions of **ABC Organization** The number of computer security incidents and the resulting cost of business disruption and service restoration rise with the increase in dependence on IT-enabled processes. Implementation of sound security policies, blocking of unnecessary access to networks and computers, improvement in user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce such risks and decrease the cost of security incidents.

## Purpose

The purpose of this document is to handle the incidents according to **ABC Organization’s** policies and procedures. This incident management policy also provides organization-wide guidance to employees on the proper response to, and efficient and timely reporting of, computer security-related incidents, such as computer viruses, unauthorized user activity, and suspected compromise of data. It also addresses non-IT incidents such as power failure. Further, this policy provides guidance regarding the need for developing and maintaining an incident management process within **ABC Organization**

## Scope

This policy applies to information systems, regardless of ownership or location, used to store, process, transmit or access **ABC Organization** Data as well as all personnel including employees, temporary workers, contractors, those employed by contracted entities, and others authorized to access **ABC Organization** enterprise assets and information resources.

## Incident Management Policy for ABC Organization

**Executive Producer.** The Executive Producer is responsible for the establishment, operation, and review of the **ABC Organization’s** Incident Management Plans, and has overall responsibility for coordinating the **ABC Organization’s** response to a critical incident, including declaring when the incident has moved from a Containment and Response phase to a Recovery and Review phase (as defined below and in the Incident Management Procedure), including a return to normal operations.

**Critical Incident Management Group (CIMG).** The CIMG is the group that will be formed in the event of a critical incident to coordinate the management of the incident. Composition is in Appendix 3 of the Critical Incident Procedure.

**Technical Lead**. Technical Leads may be prenominated through Business Continuity or Incident Response Plans ready to be enacted (for example in the case of a chemical or radiation incident) or maybe nominated on-site as the person with the specialist expertise or with sufficient authority and capacity to manage an incident occurring within the work area, especially during the confusing initial response. Technical Leads support the Critical Incident Coordinator in the overarching management of an incident with key responsibilities including establishing and taking control, assessing the situation, identifying risk, and determining priorities and communication.

**Emergency Control Team.** An Emergency Control Team provides the immediate response to an emergency (such as fire or building evacuation) that may affect the safety and health of staff and students. Their composition and responsibilities are in the HSE Emergency Management Procedure.

**Managers and Staff.** Managers must make themselves fully aware of **ABC Organization’s** Incident Management policy and procedures within their area of accountability or span of control. All staff is responsible for adherence to the compliance obligations relevant to their position; performing their duties lawfully and safely; undertaking training in accordance with the Health, Safety, and Environment requirements; and reporting and escalating compliance concerns, issues, or incidents.

All Information security incidents should be reported immediately to The IT Service Desk (via phone on ext. no. 3311, or the ServiceNow Portal), as the primary point of contact.

The report should include full and accurate details of the incident, including who is reporting the incident; what type of data is involved (not the data itself unless specifically requested); if the data relates to people, and if so, how many people are involved.

The Technical Lead is responsible for maintaining a confidential log of all information security events.

The Critical Incident Management Group (CIMG)will consider the report, and where appropriate, instigate an Emergency Control Team. IT Services will lead the Emergency Control Team and membership will depend on the type and severity of the incident. The Emergency Control Team will be responsible for investigating the circumstances and effect of the information security incident. An investigation will be started into material breaches within 24 hours of the breach being discovered, where practicable.

The investigation will establish the nature of the incident, the type of data involved, whether the data is personal data relating to individuals or otherwise confidential or valuable. If personal data is involved, associated individuals must be identified and, if confidential/valuable data is concerned, what the legal and commercial consequences of the breach may be.

The investigation will consider the extent of the sensitivity of the data, and a risk assessment performed as to what might be the consequences of its loss. This will include the risk of damage and/or distress to individuals and the institution.

The Emergency Control Team is responsible for formally documenting the incident and associated response. This information will (as a minimum) be subject to review by the **ABC Organization** Emergency Control Team with serious incidents reviewed by the Executive Producer and other senior managers

The Critical Incident Management Group (CIMG)is responsible for the initial assessment of an incident’s severity based on the scope, scale, and risk of the incident. This preliminary decision is then reviewed by the Executive Producer and/or Director of IT Strategy, Information Management, and Business Partnerships.

If at this stage the incident is deemed serious then the Emergency Control Team will be notified. If a personal data breach has occurred of sufficient scale The Emergency Control Team will notify the CIMG within the prescribed statutory time limits and manage all communications between **ABC Organization** and the CIMG.

If the breach is deemed of sufficient seriousness (in line with CIMG guidance) and concerns personal data, a notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks and will be undertaken by the Technical Lead. Liaison with the Police or other authorities may be required for serious events.

Once the incident is contained a thorough review of the event will be undertaken by the **Technical Lead**, to establish the cause of the incident, the effectiveness of the response, and to identify areas that require improvement.

Recommended changes to systems, policies, and procedures will be documented and implemented as soon as possible thereafter. Targeted training may be offered to the department affected. All information security incidents will be subject to summary review by the Emergency Control Team so that any weaknesses or vulnerabilities that may have contributed to the incident can be identified, documented, and resolved.