# Security Incident Report Manual

## Document Control

Document Owner: Chief Security Officer  
Version: 1.0  
Date: May 14, 2024  
Approval Authority: Security Management Team  
Change History: Record of updates and revisions to the document.

## Introduction

Purpose: To provide a standardized procedure for reporting, handling, and resolving security incidents to mitigate risks and ensure business continuity.  
Scope: Covers all types of security incidents affecting information systems and data security across the entire organization.  
Audience: All employees, contractors, and third-party service providers.

## Definition of Security Incidents

Types of Incidents: Data breaches, unauthorized access, malware infections, service interruptions.  
Severity Levels: Criteria for classifying incident severity from low to critical, based on impact and urgency.

## Incident Reporting Procedure

Initial Detection: Tools like IDS, firewalls, anomaly detection systems.  
Reporting Channels: Hotline numbers, email addresses, incident management systems.  
Report Content: Date and time of detection, description of the incident, affected systems, initial impact assessment.

## Incident Response Steps

Initial Response: Immediate actions like isolating affected systems.  
Investigation and Assessment: Steps for investigation, involving forensic specialists, assessing full impact.  
Resolution and Recovery: Procedures for elimination of the cause, recovery of systems, returning to normal operations.  
Documentation: Records of the incident handling process, decisions made, and rationale.

## Post-Incident Review

Review Meeting: Conducted after resolving the incident to analyze response effectiveness.  
Lessons Learned: Insights gained, documented for future reference.  
Report Update: Finalizing the incident report with comprehensive details.

## Compliance and Legal Considerations

Regulatory Reporting: Guidelines on reporting to bodies as required by laws like GDPR, HIPAA.  
Legal Implications: Overview of potential legal consequences and guidance on engaging legal counsel.

## Training and Awareness

Employee Training: Regular sessions on recognizing and reporting security incidents.  
Simulation Drills: Periodic drills to ensure preparedness.

## Appendices

A. Incident Report Form Template  
B. Contact List for Incident Response Team  
C. Regulatory Reporting Checklist  
D. Severity Level Definitions and Response Protocols

## Document Distribution and Maintenance

Distribution List: Security team, IT department, HR, legal department, top management.  
Maintenance Schedule: Review and update annually or after significant changes.