INCIDENT RESPONSE PLAN

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

INTERNAL INFORMATION

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). 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 XXXX.

Table of Contents

1. Introduction 4

1.1 Document Definition 4

1.2 Objective 4

1.3 Scope 4

1.3.1 Applicability to employees 4

1.3.1 Applicability to External Parties 4

1.3.2 Applicability to Assets 4

1.4 Reference 4

2. Plan Phases & Tasks 5

2.1 Methods of Reporting 5

2.2 Incident Response Methodology 5

2.3 Preparation 5

2.4 Detection of Incidents 6

2.5 Initial Response 6

2.6 Investigate the Incident 7

2.7 Data Collection 7

2.8 Incident Analysis 7

2.9 Incident Response Cost Analysis 8

2.10 Formulate Response Strategy 8

2.11 Incident Containment 9

2.12 Selection of a Containment Strategy 9

2.13 Incident Eradication 9

2.14 Guidelines for Incident Eradication 9

2.15 Incident Recovery 10

2.16 Selection Requirements for System Recovery 10

2.17 Guidelines for Incident Recovery 10

2.18 Additional guidelines for conducting Recovery whenever operations allow: 11

2.19 Post-Incident Activity 12

2.20 The Incident Response Team 12

2.21 Examples of Information Security Incidents 14

2.22 Classification of Information Security Events and Incidents 15

2.23 Criticality Classification 15

2.24 Incident Categories 18

3. Glossary / Acronyms 19

3.1 Glossary / Acronyms 19

4. Document Management 20

4.1 Document Revision Log 20

4.2 Document Ownership 20

4.3 Document Coordinator 20

4.4 Document Approvers 20

4.5 Document Distribution 20

5. Appendix A – Information Security Incident Response Form 21

# Introduction

## Document Definition

This document is a Procedure.

For a full description of document types, see *XXXX-PRC-ALL-001 - Information Security Policy Framework*.

## Objective

The purpose of this process provides a structured and planned approach to:

* + - * Define appropriate procedures for responding to information security incidents
      * Detect, report and assess information security incidents.
* Provide practical guidance on responding to incidents effectively and efficiently. This guide establishes an Incident Response Capability (IRC).
  + - * Resolve the information security event or issue in a timely manner
      * To ensure that proper post-incident reporting occurs and that procedures are reviewed and adjusted to mitigate risk and prevent future incidents.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Procedure applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This procedure applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Reference

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-012 – Incident Response Policy*

# Plan Phases & Tasks

## Methods of Reporting

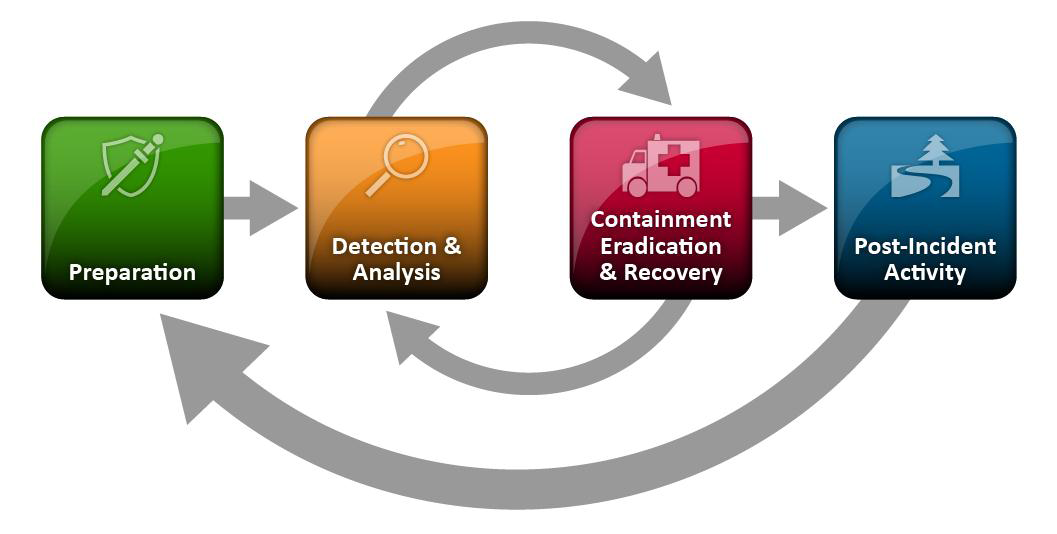
All employees and users are responsible for promptly reporting suspected or known security incidents, including an observed or suspected security weakness in the XXXX’s systems or services, in accordance with the XXXX-POL-ALL-012 - Incident Response Policy

There are various ways in which security incident breaches can be reported. We recommend security incidents/breaches to be recorded through the following:

* Send a mail to [helpdesk@XXXX.com](mailto:helpdesk@zenith-bank.co.uk), the help desk portal through the incident response form (see Appendix A below) or call extension 1234.
* All suspected high severity incidents, including those involving possible breaches of the XXXX’s information, must be reported directly to the Head IT/Information Security Officer as quickly as possible by phone (preferred), email, or in person.

## Incident Response Methodology

Information security incidents are often complex, multifaceted problems. The components of incident response include:



**Figure 1: Components of Incidence Response**

## Preparation

Taking actions to prepare the organization and the IRT before an incident occurs. The preparation phase comprises the onlyproactive measures the IRT can initiate to ensure that the organization’s assets and information are protected. Ideally, preparation will involve not just obtaining the tools and developing techniques to respond to incidents, but also taking actions on the systems and networks that will be part of any incident that needs to be investigated.

* + - Implementing host-based & network-based security measures
    - Employing an intrusion detection system (IDS)
    - Creating strong access control
    - Performing timely vulnerability assessments
    - Ensuring backups are performed on a regular basis
* The hardware, software, documentation needed to investigate computer security incidents
* The appropriate policies and operating procedures to implement the response strategies
* The training of staff or employees required to perform incident response in a manner that promotes successful forensics, investigations, and remediation

## Detection of Incidents

This stage identifies a potential Information security incident. Information security incidents are normally identified when someone suspects that an unauthorized, unacceptable, or unlawful event has occurred involving an organization’s computer networks or data-processing equipment.

This can be reported by an end user, detected by a system administrator, identified by IDS alerts, Information Security Analyst, HCM, or discovered by many other means. Regardless of how an incident is detected, it is paramount to record all of the known details. It is imperative to use an initial response checklist to make sure the pertinent facts are properly documented. The initial response checklist should account for many details, not all of which will be readily discernable immediately after an incident is detected.

Some of the critical details include the following:

* Current time and date
* Who/what reported the incident
* Nature of the incident
* When the incident occurred
* Hardware/software involved
* Points of contact for involved personnel

## Initial Response

One of the first steps of any investigation is to obtain enough information to determine an appropriate response. The details surrounding the incident are documented by whoever detected the incident or by an individual who was notified that the incident may have occurred (for example, help desk or security personnel). The control of the response should be forwarded to the IRT early in the process to take advantage of the team’s expertise.Typically, the initial response will not involve touching the affected system(s). This phase involves the following tasks:

* Assembling the IRT
* Verify that an incident has actually occurred, which systems are directly or indirectly affected, which users are involved, and the potential business impact
* Interviewing system administrators who might have insight into the technical details of an incident
* Interviewing business unit personnel who might have insight into business events that may provide a context for the incident
* Reviewing intrusion detection reports and network-based logs to identify data that would support that an incident has occurred
* Reviewing the network topology and access control lists to determine if any avenues of attack can be ruled out
* Verify enough information about the incident so that the actual response will be appropriate

## Investigate the Incident

The investigation phase involves determining **who**, **what**, **when**, **where, how**, and **why** surrounding an incident. Investigation and reviews of host-based evidence, network-based evidence, and evidence gathered via traditional, nontechnical investigative steps is carried out. An information security investigation shall be divided into two phases: data collection and analysis. During the data collection phase, relevant information needed to resolve the incident shall be collected.

In the analysis phase, all the data collected is examined to determine who, **what, when, where,** and **how** is the information relevant to the incident.

## Data Collection

Data Collection is a parallel process that runs throughout the Incident Management Lifecycle. All phases of incident management require detailed documentation of actions taken and the conclusions drawn from analysis. This assists in determining the correct response and in supplying vital data for conducting follow‐up investigation and producing the post‐incident report. The data collected will form the basis of the conclusion. Evidence must be handled with care

Collection shall include any information that is associated with a specific incident, including the following:

* All computer or relative non‐IT data, including host and network logs, forensics images, IDS logs, Consensual monitoring logs, pen registers, backup logs, and any other data or documentation that provides information about the compromised system(s) or file(s);
* All actions the incident response team initiates;
* Records of conversations with all employees; and
* Any other auditing information produced by software tools, log files, and similar data
* All evidence collected are kept in the folder Y:\Incident Reports\Incident Evidence.

## Incident Analysis

Analysis of incident responses is critical to determining how to protect against and minimize the impact of future occurrences and to assess how well the XXXX responded to the incident. Questions for consideration in gathering information for analysis and reporting of the incident are as follows:

* What are the details of the incident and what was done to neutralize the effects of the incident? Answers to this question may be used to capture important details in addition to those recorded in the incident log.
* Was there enough preparation for the incident by users, computer specialists, and managers?
* Did detection and response processes and procedures work as intended? If not, where did they not work? Why did they not work?
* Was the incident detected in real‐time or near real‐time?
* Are there incident detection tools, methods of discovery, monitoring procedures, or improvements in these areas that would have improved the capability to detect the incident?
* Was the incident sufficiently contained, and are there response improvements that would have enhanced containment of the incident?
* Were methods to collect evidence sufficient to support a successful investigation and future litigation by law enforcement? Could correction procedures have been improved for a more effective recovery?
* What practical difficulties were encountered in responding to the incident?
* Are there updates to policies and procedures that would have enabled a more effective response and recovery?
* Were communications procedures, internal and external, adequate throughout the detection and response processes? Was there enough preparation for the incident?
* Did detection occur promptly or, if not, why not?
* Could additional tools have helped the detection and eradication process? Was the incident sufficiently contained?
* Was communication adequate, or could it have been better? What practical difficulties were encountered?

## Incident Response Cost Analysis

An important consideration in post‐incident analysis is the determination of financial costs associated with the incident response capability. This would not only assist in assessing damage for prosecution, but would also demonstrate the importance of expenditures associated with information systems security. Examples of costs that are typically included in incident response cost analysis are:

* Costs of damaged computer system assets. (Recommend conducting an inventory of the affected computer system assets, not only to discover and determine the cost of damaged assets, but also to provide assurance of the integrity of undamaged assets.);
* Monetary cost associated with employees’ time required to deal with the incident;
* Cost due to lost operations;
* Estimated value of any compromised sensitive information assets

## Formulate Response Strategy

Response strategies will vary based on the circumstances of the information system security incidents The following factors need to be considered when deciding how many resources are needed to investigate an incident, whether to create a duplication of relevant systems, whether to make a criminal referral, whether to pursue civil litigation, and other aspects of the response strategy: The response strategy should be approved by top-level management. Options should be quantified with pros and cons related to the following:

* How critical are the affected systems?
* How sensitive is the compromised or stolen information?
* Estimated financial loss
* Network & User downtime and its impact to operations
* Whether or not the organization is legally compelled to take certain actions
* Public disclosure of the incident and its impact to the organization’s reputation/business
* Theft of intellectual property and its potential economic impact

## Incident Containment

The overall purpose of Incident Containment is to limit the damage that an incident may cause while at the same time causing the least possible impact to mission‐critical processes. The Containment phase of the Incident Management Lifecycle requires critical decision‐making (e.g., determining whether to shut down a system, disconnect it from the network, monitor its activity, or disable functions such as remote file transfer) and consists of short‐term, planned actions that may remove access to compromised systems, limit the extent of current damage to a system, and prevent additional damage from occurring. The specific steps that should be followed depend on the type of incident (intrusion, virus, theft, etc.), and whether the incident is in progress (e.g., an intrusion, disruption of service) or is discovered after the attack.

## Selection of a Containment Strategy

When an Information Security incident affects mission‐critical information or computing services, especially those “High” System Security Classifications, the IRM in consultation with the ISO, and other key affected parties shall decide how to address the incident while at the same time minimizing impact to mission‐critical processes. In the case of a low‐risk incident, the IRM may decide to move quickly to eradicate the incident without shutting down the affected system.

In the case of a high‐risk incident affecting a system with sensitive information or applications, the IRM may direct that the system be shut down or at least be temporarily isolated from the network. If there is a reasonable chance that letting a system continue to run as normal without risking serious damage, disruption, or compromise of data, or to identify a perpetrator, the IRM may determine that operations can continue under close monitoring.

## Incident Eradication

Eradication is the application of sufficient technical measures on an affected system to eliminate the causes and effects of an intrusion or attack to a point where the risk of re‐emergence of the cause is reduced to zero or mitigated to a minimal or acceptable level. Once all containment procedures and actions have been completed, and all data which may be useful to performing an ongoing analysis of the compromise is collected, eradication may proceed.

## Guidelines for Incident Eradication

* **Review Incident Analysis**:Data collected and analyzed shall be used to understand the exploited vulnerability and mayinform the minimum requirements for eradication.
* **Perform a Vulnerability Analysis:** A vulnerability analysis tool (such as an automated vulnerability assessment tool) shall beused to scan exposed systems, services, and applications that are connected to the affected systems. Special attention may be paid to web servers/services, databases, or other complex architectures such as Service Oriented Architectures (SOA), mainframes, and e‐commerce systems.
* **Improve Security Controls on the affected System and other Systems**:Appropriate protection techniques shall beimplemented in the environment where appropriate. These techniques may consist of activities such as: applying security patches, changing the system name or IP address, securing and protecting boundary defense hardware and software, implementing Network Admission Control (NAC), implementing two‐factor authentication, or in extreme cases, porting the machine's functions to a more secure operating system.
* **Focus on Removing Malignant Artifacts**:The IRT shall concentrate on the eradication of malignant artifacts (e.g., Trojanhorses), and may concentrate on the eradication of benign artifacts if they present serious risk.
* **Thoroughly Remove Artifacts From all Media**:The ISO, or designee, shall ensure that all malicious artifacts are removedfrom all systems and media (including CD‐ROMs and backup media) by using one or more proven commercial eradication applications or by manual surgical removal following an in‐depth malware analysis which has identified the entirety of the malware package or by re‐baseline the affected host.

## Incident Recovery

Recovery is defined as restoration of affected information systems to normal operational status. The recovery phase procedures for resumption of normal operations contained in this section provide a framework for use when recovering from an incident. The recovery process begins when the cause of the incident has been eradicated or mitigated to a degree of risk determined to be acceptable by the CISO and the IRM.

## Selection Requirements for System Recovery

* For systems categorized moderate security classification, if the analyses conducted has provided a high degree of confidence that the incident did not affect the software or the information stored on the system, then there may only be a minimal amount of effort required to provide assurance that the system is properly recovered. In this case, only simple countermeasures shall be needed to protect the system against future occurrences.
* If the system has a high security classification, or in a case where the analyses conducted has not provided a high degree of confidence that the incident did not affect the system software or data, then there may be a more complex recovery solution requiring a complete restoration of the system to a normal operating condition.

## Guidelines for Incident Recovery

* **Document the Recovery Phase**:Documentation of the recovery steps can assist in maintaining focus as the recoveryprocess proceeds. All documentation associated with the incident shall be noted in the incident report for later review and reporting.
* **Decide the System Restoration Procedure**:Several restoration options may be available depending on the severity of theincident, the sensitivity of the system affected, and the backup systems available. The selection of the best option may require the involvement and authorization of the application/data owner, the CISO, and/or senior management.
* **Validate Data Restored from Untrustworthy Sources**:In restoring files other than the operating system and applicationsfiles, only the most trusted backup files shall be used. Restored system data and user files shall be investigated for altered data or other signs of compromise.
* **Validate the Restored System before Returning to Service**:Validation of the restored system shall be performed byexecuting a known series of development tests when prior test results are available for comparison. Prior to restoration of network connectivity, the ISO shall verify that all known vulnerabilities have been mitigated.
* **Get Authorization and Communicate with Users before Restoring Service**:Before reconnecting the recovered system tothe network to resume normal operations, the ISO shall obtain authorization from the IRM and notify any organizations that would be affected.
* **Conduct a review of the security controls:** The IRM shall verify that the system is configured in accordance with thecurrent configuration management guidelines; that logging, auditing, and accounting programs are functional; and any security tools are functioning. The ISO is responsible for ensuring discrepancies are corrected.
* **Monitor the Restored System**:So as to maintain a high-level confidence in the security of the restored system it shall bemonitored to prevent additional intrusion, or a recurrence of the incident. Any knowledge gained through analysis should be used to provide insight into an attacker’s techniques and/or methods to develop better monitoring techniques. Some items to be monitored may include: failed login attempts, attempts to access back doors, attempts to re‐exploit the original vulnerability, and attempts to exploit any new vulnerabilities of the system.

## Additional guidelines for conducting Recovery whenever operations allow:

* **Only Perform “Rapid Restoration” When Mission‐Critical**:If it is decided to return to operation or maintain the affectedsystem in operational use without completion of the recovery process due to mission‐critical requirements, the recovery process may continue in parallel with operational use. Incident analysis and the elimination of vulnerabilities should continue in parallel with rapid restoration to mitigate the risk further incidents.
* **Replace the Affected System with a Backup System When Possible**:Employment of a backup system for operational usewhile the affected system is under examination may be permissible. Because data stored to backup may already be contaminated before the incident is actually reported and addressed, backup tapes shall be carefully examined to ensure the integrity of the data. The compromised system should first be isolated from the network and from all backup systems. The backup system data may then be restored from trusted system backup files rather than using possibly contaminated data files from the affected system. If system mirroring is employed, backup tapes shall be examined to determine at what point the restore should occur in order to ensure the integrity of the data restoration process.
* **Restore the System Offline Whenever Operations Allow**:Restoration of the operational system while it is kept off‐linemay provide the greatest opportunity for recovery of incident data and for determining the cause and extent of the incident. Operating the system in a stand‐alone, single user status may prevent other users, intruders, and malicious processes from accessing or changing the compromised system.

## Post-Incident Activity

Performing post‐incident activity is a critical step in responding to an incident. Post‐incident activities enable the IRT and other employees to learn from the successful and unsuccessful actions taken in response to an incident. Capturing, documenting, and disseminating what worked, and what did not, will help to reduce the likelihood of similar incidents re‐occurring. The level of effort required for Follow‐Up activities should reflect the scope and impact of the incident.

* **Post Incident Analysis -** So that critical details can accurately be recalled and recorded; a post‐incident analysis shall begin as soon as possible. An after‐ action meeting with all involved parties shall be convened to disseminate details of the incident, address incident response procedures, and to obtain an estimate of costs resulting from the incident. Vulnerabilities uncovered during the incident response and analysis shall be remedied and a decision shall be reached as to whether or not to conduct a new system risk analysis.
* **Post Incident Report -** Information gathered during the incident post‐analysis, as well as any other pertinent information, shall be included in an incident response report generated for the incident. The IRT shall prepare a report, including any "lessons learned" and cost analyses, which may be used to further staff awareness (without endangering security mechanisms) and/or can be used in training.
* **Taking Action**

Occasionally, the XXXX will need to take action to discipline an employee or to respond to a malicious act by an outsider. When such incident warrants, this action can be initiated with a criminal referral, a civil complaint, or some administrative reprimand or privilege revocation. Disciplining or terminating employees via administrative measures is currently more common than initiating civil or criminal actions. Some administrative actions that can be implemented to discipline internal employees include the following: Letter of reprimand, Immediate dismissal, Mandatory leave of absence for a specific length of time (paid or unpaid), Reassignment of job duties (diminished responsibility), Temporary reduction in pay to account for losses/damage, Public/private apology for actions conducted, Withdrawal of certain privileges, such as network or web access.

* **Revising Policies, Procedures, and Security Plans**

The lessons learned report, derived from incident handling activities, may be incorporated into information security policies, procedures, and security plans, training, and testing/exercises and the resulting changes implemented. Based on incident analysis and reporting, corrective actions may be developed and implemented to help prevent any recurrence of the incident, or to more effectively handle a recurrence.

## The Incident Response Team

The Incident Response Team is responsible for managing the XXXX’s response to an incident and how the XXXX interacts with third parties such as law enforcement agencies, regulatory bodies, customers, employees and the media. The XXXX’s incident team shall be trained periodically as needed.

The Incident Response Team structure shall be made up of representatives of the following:

|  |  |
| --- | --- |
| Role | Responsibility |
| Team Leader/ Deputy Team Leader | * Initiates response * Assembles incident team * Overall management of the incident response team * Acts as interface with the board and other high-level stakeholders |
| Team Facilitator | * Supports the incident response team leader * Co-ordinates resources within the command centre * Prepares for meetings and takes records of actions and decisions * Briefs team members on latest status on their return to the command centre |
| Incident Liaison | * Attends the site of the incident as quickly as possible * Provides the IT expertise to assesses the extent and impact of the incident * Liaises with the IRT on an ongoing basis to provide IT related updates and answer any questions required for decision making by the IRT |
| Information Technology | * Provides input on technology related issues * Assists with impact assessment |
| Business Operations | * Contributes to decision-making based on knowledge of business operations, products and services * Briefs other members of the team on operational issues * Helps to assess likely impact on customers of the organization |
| Facility Management | * Deals with aspects of physical security and access * Provides security presence if required. |
| Health and Safety | * Asses the risk to life for the incident * Ensures that legal and responsibilities for health and safety are met * Liaises with emergency services such as police, fire and medical * Considers environmental issues with respect to the incident |
| Human Resources | * Assesses and advises on HR policy and employment contact matters * Represents the interest of XXXX’s employees |
| Business Continuity Planning | * Provide advice and invoke business continuity plans if required |
| Communications | * Responsible for ensuring internal communications are effective * Decides the level, frequency and content of communications with external parties such as the media\Defines approach to keeping affected parties informed * Monitors external information feeds such as news |
| Legal, Regulatory and Compliance | * Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks * Assesses the actual and potential legal implications of the incident and subsequent actions |

The IRT will consist of the following people in the roles specified.

|  |  |  |
| --- | --- | --- |
| Name | Department | Number |

Depending on the seriousness and impact of an information security incident it may be necessary to mobilize all or only part of the Information Security Incident Response Team.

## Examples of Information Security Incidents

Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

* Giving information to someone who should not have access to it - verbally, in writing or electronically.
* Sending a sensitive e-mail to 'all staff' by mistake.
* Receiving unsolicited mail of an offensive nature.
* External cyber attacks not limited to DDOS, ransomware, worms, trojans, phishing etc
* Receiving unsolicited mail which requires you to enter personal data.
* Core information system failures and loss of service
* Finding data that has been changed by an unauthorised person.
* Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
* Unknown people asking for information which could gain them access to XXXX’s data (e.g. a password or details of a third party).
* Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
* Theft / loss of any company’s computer equipment.
* Theft of equipment, data or information, fraud or fraudulent activities;
* Attempts (either failed or successful) to gain unauthorized access to data or information stored on computer systems e.g. hacking;
* Changes to information or data or system hardware, firmware, or software characteristics without the company’s knowledge, instruction, or consent e.g. malware (viruses, Trojans etc.)
* Use of unapproved or unlicensed software on the company’s equipment
* Unwanted disruption or denial of service to a system e.g. spam attacks; receiving unsolicited mail of an offensive nature; receiving and forwarding chain letters – including virus warnings, scam warnings and other emails that encourage the recipient to forward onto others
* Accidental loss of equipment, data or information including handheld devices such as Blackberries;
* Human error e.g. emailing sensitive information outside of the company’s network either in error or without appropriate security measures in place;
* Sharing/transfer of data or sensitive information with those who are not entitled to receive that information
* Sharing more than the necessary amount of personal/sensitive information to complete required tasks;
* Accessing computer systems/applications using someone else’s authorization e.g. user id and password; Sharing access tokens or logins
* Unforeseen circumstances e.g. fire or flood;
* Unsecure premises

## Classification of Information Security Events and Incidents

It is important to document information security incidents in a consistent manner, in order to share the information on information security incidents, make it easier to automate incident reporting and responses, and identify the severity levels of information security incidents using consistent criteria. This provides the guidelines needed for Incident Response Managers (IRM) to classify the incident category, criticality level, and sensitivity level for each incident. This information will be entered into the help desk portal when an incident is created.

## Criticality Classification

The criticality matrix defines the minimal user response time and ongoing communication requirements for an incident.  The criticality level should be entered into the helpdesk portal when an incident is created, and it should not be altered at any point during the incident lifecycle except when it was incorrectly classified in the first place.   Typically, the IRM will determine the criticality level.  In some cases, it will be appropriate for the IRM to work with the user to determine the criticality level. Classifying information security incidents will depend on several factors such as;

* The nature of the incident.
* The criticality of the systems being impacted.
* The number of systems impacted by the incident.
* The impact the incident can have on the organization from a legal and public relations point of view.
* Legal and regulatory requirements.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Criticality Level** | **Criticality Level Definition** | **Typical Incident Categories** | **Initial Response Time** | **Ongoing Response (Critical Phase)** | **Ongoing Response (Resolution Phase)** | **Ongoing Communication Requirement** |
| S1 | Incident affecting critical systems or information with potential to be revenue or customer impacting or may result in criminal charges, regulatory fines or in damage to the XXXX’s reputation. | * Denial of service * Compromised Asset (critical) * Core XXXXing Information system failures and loss of service * Internal Hacking (active) * External Hacking (active) * Virus / Worm (outbreak) * Destruction of property (critical) * Compromise of information resulting in serious data disclosure * Serious breaches of the organization’s Acceptable Usage Policy | 30-60 Minutes | Team Leader to initiate a full incident response on 24x7 basis. | Team Leader to ensure work assigned to relevant parties are concluded during normal business hours. | Incident update sent to appropriate parties on a daily basis during critical phase.  If IRT involvement is necessary to restore critical systems to service then incident update will be sent a minimum of every 2 hours.  Incident update sent to appropriate parties on a weekly basis during resolution phase. |
| S2 | Incident affecting non-critical systems or information, not revenue or customer impacting. Employee investigations that are time sensitive should typically be classified at this level. | * Internal Hacking (not active * External Hacking (not active) * Information system failures and loss of service(Not Active) * Unauthorized access. * Policy violations * Unlawful activity. * Compromised information. * Compromised asset. (non-critical) * Destruction of property (non-critical) | 3-12 Hours | Deputy Team Leader and Team Facilitator to coordinate resolution on 24x7 basis. | Deputy Team Leader and Team Facilitator to ensure resolution activities are completed during normal business hours. | Incident update sent to appropriate parties on a daily basis during critical phase.    Incident update sent to appropriate parties on a weekly basis during resolution phase. |
| S3 | Possible incident, non-critical systems.  Incident or employee investigations that are not time sensitive.  Long-term investigations involving extensive research and/or detailed forensic work. | * Email * Forensics Request * Inappropriate use of property. * Policy violations. | 48 Hours | Incident is assigned to relevant parties by Deputy Team Leader and Team Facilitator to resolve | Incident is assigned to relevant parties by Deputy Team Leader and Team Facilitator to resolve | Incident update sent to appropriate parties and Team Leader on a weekly basis |

## Incident Categories

All incidents managed by the IRT should be classified into one of the categories listed in the table below.

|  |  |  |
| --- | --- | --- |
| **Incident Category** | **Sensitivity\*** | **Description** |
| Denial of service | S1 | * DOS or DDOS attack. |
| Forensics | S1 | * Any forensic work to be done by IRT. |
| Compromised Information | S1 | * Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property. |
| Compromised Asset | S1 | * Compromised host (root account, Trojan, rootkit), network device, application, user account.  This includes malware-infected hosts where an attacker is actively controlling the host. |
| Unlawful activity | S1 | * Theft / Fraud / Human Safety / Child Porn.  Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention. |
| Internal Hacking | S1, S2, S3 | * Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware. |
| External Hacking | S1, S2, S3 | * Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware. |
| Malware/Virus | S1 | * A virus or worm typically affecting multiple corporate devices.  This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset) |
| Email | S2 | * Spoofed email, SPAM, and other email security-related events. |
| Consulting | S3 | * Security consulting unrelated to any confirmed incident. |
| Policy Violations | S2 | * Sharing offensive material, sharing/possession of copyright material. * Deliberate violation of Information security policy. * Inappropriate use of corporate asset such as computer, network, or application. * Unauthorized escalation of privileges or deliberate attempt to subvert access controls. |
| \* Sensitivity will vary depending on circumstances. | | |

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| IR | Incident Response |
| IRT | Incident Response Team |
| PD | Personal Data |
| SPD | Sensitive Personal Data Exposure |
| PCI | Payment Card Industry |
| IRM | Incident Response Manager (Information Security officer) |
| US-CERT | United States Computer Emergency Readiness Team |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Document Distribution

The Document Owner controls distribution of this document.

* All Staff

# Appendix A – Information Security Incident Response Form

|  |  |
| --- | --- |
| **Contact Information** | *To be completed by the* ***affected user*** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | |  |  | |
| Name: | Click here to enter text. | | | | Position: | Click here to enter text. | |
|  | | | | | | | |
| Report Date: | Click here to enter text. | | | | Helpdesk Incident ID: | Click here to enter text. | |
|  | | | | | | | |
| Report Status: | | Initial Report **☐** | | | Follow-up Report **☐** | | Final Report: **☐** |
| |  |  | | --- | --- | | **Incident Information** | *To be completed by the* ***affected user*** | | | | | | | | |
|  | | | | | | | |
| Type of Incident:  (e.g. Malware, Loss or Theft of Equipment, Phishing Email, Improper Usage, Other) | | | | Click here to enter text. | | | |
|  | | | | | | | |
| Date and Time Incident Detected: | | | | Click here to enter text. | | | |
|  | | | |  | | | |
| Date and Time Incident Occurred: | | | | Click here to enter text. | | | |
|  | | | |  | | | |
| Incident Location:  (e.g. Cornhill, Dubai, Home) | | | | Click here to enter text. | | | |
|  | | | |  | | | |
| Reported to: | | | | Click here to enter text. | | | |
| |  |  | | --- | --- | | **Description** | *To be completed by the* ***IT Department****.* | | | | | | | | |
|  | | | | | | | |
| Description:  (Give the details of what happened and what was affected.) | | | Click here to enter text. | | | | |
| |  |  | | --- | --- | | **Impact and Severity** | *To be completed by the* ***IT Department*** | | | | | | | | |
|  | | | | | | | |
| Impact and Severity:  (What was the full impact and severity of the incident?) | | | Click here to enter text. | | | | |
| |  |  | | --- | --- | | **Root Cause Analysis** | *To be completed by the* ***IT Department*** | | | | | | | | |
|  | | | | | | | |
| Root Cause Analysis:  (What was the root cause of the incident?) | | | Click here to enter text. | | | | |
| |  |  | | --- | --- | | **Mitigation** | *To be completed by the* ***IT Department*** | | | | | | | | |
|  | | | | | | | |
| Mitigation:  (What has been done to prevent or reduce the severity of future incidents?) | | | Click here to enter text. | | | | |
| |  |  | | --- | --- | | **Recommendation** | *To be completed by the* ***IT Department*** | | | | | | | | |
|  | | | | | | | |
| Recommendation:  (Follow-up actions recommended to be taken.) | | | Click here to enter text. | | | | |
| |  |  | | --- | --- | | **Additional Comments/Notes** | *To be completed by the* ***IT Department*** | | | | | | | | |
|  | | | | | | | |
| Comments/Notes | | | Click here to enter text. | | | | |
|  | | | | | | | |

*Report approved by:*

|  |  |  |  |
| --- | --- | --- | --- |
| Name: | Click here to enter text. | Date: | Click here to enter text. |