HSE Ireland Incident Response Plan

[HSE-IR-PLN-2024]

Prepared by: Gaurav Suryawanshi

as a part of

CYBERSEC 510.02. Fa24

Document Control Section	
Document Title	Incident Response Plan
Document Number / Internal Code Reference	HSE-IR-PLN-2024
Classification	TLP: AMBER (Limited Disclosure)
Location	HSE Master -> SOP Files OneDrive

Authorization		
Document Owner	**Reviewed By**	**Approved By**
ITIS, IS Steering Committee, IRT (co-owner)	Gaurav Suryawanshi (self)	Gaurav Suryawanshi (self)

Review/Amendment/Changelog				
Version	**Modification Date**	**Section**	**A/M/D**	**Brief Description of Change/Review (performed by – details)**
v0.1	16th October, 2024	1-7	n/a	Plan creation

Table of Contents

1. INTRODUCTION

This document outlines the plan and strategy for addressing information security incidents at the HSE. It outlines the duties and obligations of those involved, incident classification, connections to other policies and playbooks and reporting criteria. The main objective of this Incident Response Plan (IRP) is to identify and respond to information and cyber security incidents, assess their extent and risk, take appropriate action, communicate the findings and risks to all stakeholders, and minimize the chances of the incident recurring.

1.1 SCOPE

The following plan pertains to the servers, systems, applications, networks, and data of the HSE. Its scope encompasses any individual or device with access to any system, network, or data that is operated or supported by HSE.

1.2 GOALS

The primary objectives of this plan are as follows:

Proactive Goals:

- Ensure the integrity of critical information assets.
- Detect and respond to intrusions, misuse, and other negative events.
- Recover systems, data, and services in the event of a disruption.
- Contain intrusions and negative incidents.

Reactive Goals:

- Investigate the source or cause of an incident.
- Manage communication with internal and external agencies.
- Conduct investigations in a manner that supports prosecution, where appropriate.
- Establish and follow a procedure for reporting suspicious activity.

Reactive Proactive Goals:

- Enable trend analysis, ongoing risk assessment, and mitigation.
- Educate the Incident Response Team (IRT).
- Heighten awareness among relevant team members.
- Update the Decision Tree as necessary.

1.3 PRIORITIES

The following priorities are fundamental to defining HSE's information security response:

- Safeguarding customers' information and ensuring the integrity of company-wide data.
- Upholding the reputation of the HSE and regulating external communication.
- Preventing harm to systems.
- Minimizing disruption to computing resources.

1.4 MAINTENANCE

The Head of the Information Technology and Information Security Department (ITIS) will assume responsibility for tracking the changes and updating this document.

2. DEFINITIONS

Events

Events in IT refer to any exceptions to the normal operation of infrastructure, systems, or services. It's important to note that not all events escalate to become incidents.

Incident

On the other hand, an incident is an event that, upon assessment by the IT security team, breaches the Acceptable Use Agreement or other relevant policies, standards, or code of conduct. Such incidents pose a threat to the confidentiality, integrity, or availability of Information Systems or agency data.

Incidents may come to light through various channels such as network and server monitoring systems, service disruptions or outages, as well as reports from internal staff or external organizations. Once identified, incidents are to be officially declared and documented via electronic mail or an IT Ticket/Documentation System.

Complete IT service outages can also result from security-related incidents. Procedures for handling service outages are outlined in the Business Continuity Plan.

Incidents will be classified based on their potential for exposing sensitive or restricted data, or the criticality of affected resources, using a severity rating detailed later in this document. The initial severity rating may be adjusted during plan execution.

Detected vulnerabilities will not be considered incidents. The ITIS Department utilizes tools to scan HSE's network environment and, depending on the severity of the identified vulnerabilities, may alert affected users, disconnect affected machines, or implement other mitigations. In the absence of indications of sensitive data exposure, vulnerabilities will be reported to the Director of IT, and potential technological solutions will be explored to minimize the associated risk.

Personally Identifiable Information (PII)

In order to comply with security breach notification requirements, personally identifiable information (PII) is defined as an individual's first name or first initial and last name combined with any of the following data elements:

- Social security number
- State-issued driver's license number
- State-issued identification card number
- Financial account number along with a security code, access code, or password that would grant access to the account
- Medical and/or health insurance information

3. ROLES AND RESPONSIBILITIES

Director of IT

The Director of IT, in collaboration with the Head of ITIS (Information Technology & Information Security), is responsible for determining whether an incident requires immediate action, warranting an emergency meeting of the IRT, or if it is a minor incident that needs to be reviewed during a IRT meeting.

Chief Information Security Officer (CISO)

Additionally, as HSE's Chief Information Security Officer, the Director of IT may engage an IT security consulting company to provide virtual CISO services. This involves enlisting a highly qualified information security consultant familiar with HSE's computing environment, IT staff, and processes. The CISO will play a crucial role in the event of a cyber-security incident by:

- Identifying the physical and electronic evidence to be collected as part of the Incident Investigation.
- Overseeing and gathering forensic evidence and acting as the liaison between HSE and law enforcement.
- Providing guidance throughout the response process, including coordinating forensic investigations and communicating with law enforcement.

Incident Commander (IC)

Depending on the nature of the incident, a team of HSE's Systems and/or Network Engineers (part of their internal Incident Response Team/unit) will report to an Incident Commander who will be responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation. This is referenced in the [HSE-IR-POL-2024] document.

Incident Response Team (IRT)

The Incident Response Team consists of specialized members of the IT Division staff or outside contractors who gather, preserve, and analyze evidence so that an incident can be concluded.

Insider Threats

Insiders refer to current or former employees, contractors, or business partners who have access to sensitive data and may misuse their access to jeopardize the confidentiality, integrity, or availability of HSE's IT information or systems. This threat necessitates specific organizational and technical adjustments to the Incident Response Plan, as outlined below.

Law Enforcement

Law Enforcement encompasses federal and state law enforcement agencies, as well as U.S. government agencies that issue warrants or subpoenas for the disclosure of information. Any interactions with these entities will be managed in coordination with HSE's Legal Counsel.

Legal Counsel

HSE's Legal Counsel will serve as the intermediary between HSE's Cybersecurity Leadership, the incident response team (IRT) and external Law Enforcement agencies. They will also offer guidance on the scope and manner of all disclosures to law enforcement and the public.

Users

Users are individuals, stakeholders or employees within the HSE community or anyone accessing an Information System, Data, or HSE networks who may be impacted by an incident.

4. METHODOLOGY

The methodology outlined in this plan denotes the fundamental tasks for Incident Response and may be complemented by specific internal guidelines and procedures governing the utilization of security tools and communication channels. These internal guidelines and procedures are subject to modification in response to technological advancements.

Staffing for an Incident Response Capability

The ITIS Department will deploy its internal staff and may engage third-party augmentation, such as external security consulting services, to thoroughly investigate each incident and communicate its status to relevant parties, while concurrently monitoring the tools that identify new events.

Training

Continuous improvement of incident handling processes necessitates periodic review, testing, and translation into recommendations for enhancements. The ITIS staff will receive periodic training on procedures for reporting and handling incidents to ensure consistent and appropriate responses, and to integrate post-incident findings into procedural enhancements.

Intrusion Detection Procedure

• All HSE employees will receive training in "broadcast awareness," requiring them to promptly alert all relevant individuals of suspicious activities in real time. Any suspected and/or confirmed instances of attempted and/or successful intrusions must be immediately reported to the IT department.
• The IT department members will be trained by the Director of IT on how to report potential issues to the IRT for investigation while troubleshooting and maintaining HSE's systems.
• The Director of IT will meticulously assess all incidents to determine appropriate action and ensure compliance with necessary reporting requirements. Reporting based on system availability and customer information breach is outlined below.
• Depending on the nature and scope of the incident, technical staff and the Director of IT will decide whether the incident can be resolved locally or if additional assistance is required from the IRT or other external sources.
• Audit logging processes for operating systems, user accounts, and application software must be enabled on all host and server systems.
• Alarm and alert functions of firewalls and other network perimeter access control systems must be enabled.

5. INCIDENT RESPONSE PHASES

According to the NIST SP 800-61 (Computer Security Incident Handling Guide), HSE's IT response to a Cyber Security Incident is guided by six phases: Assessment, Detection, Containment, Investigation, Remediation and Recovery, and Post-incident follow-up. One of the crucial phases is Remedial and Containment Action, which involves taking necessary steps to address and contain the incident effectively.

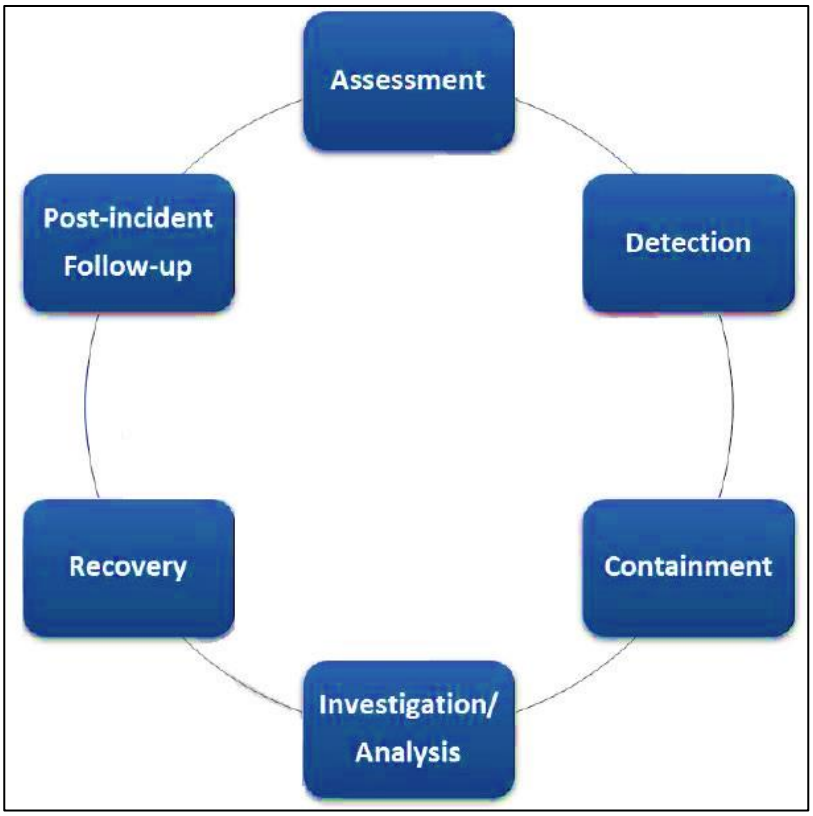


Figure 5.1 – The 6 IR phases as per NIST SP 800-61

1. Assessment

During the Assessment phase, it is crucial to confirm whether an incident is a genuine threat or a false positive. This involves obtaining an understanding of the type and severity of the attack. Detailed records of actions taken must be maintained for future documentation of the incident, whether real or false.

2. Detection

Detection involves the identification of security events through tools or notification by internal or external sources regarding a suspected incident. This phase encompasses the declaration and initial classification of the incident.

3. Containment

In the Containment phase, a prompt response is essential in mitigating the impact of a security incident. The response plan prioritizes the protection of human life and safety, safeguarding client and agency data, protecting hardware and software, and minimizing disruption of computing resources. The Director of IT will invoke appropriate measures based on the specific situation at hand.

As a starting point, however, the following will be the priority of the response plan:

1. Protect Client and Agency data - including proprietary, sensitive, and managerial data.
2. Protect hardware and software against attack. This includes protecting against loss or alteration of system files and physical damage to hardware.
3. Minimize disruption of computing resources. Although uptime is very important in HSE's environment, keeping systems up during an attack might result in greater problems. For this reason, minimizing disruption of computing resources should be a lower priority than protecting agency data and systems.

4. Investigation & Analysis

To effectively recover from an attack, it is crucial to assess the extent of the compromised systems. This assessment will impact containment and risk mitigation efforts, recovery strategies, communication plans, and the consideration of legal action. An attempt will be made to:

- Determine the nature of the attack (this might be different than the initial assessment suggests).
- Determine the attack point of origin.
- Determine the intent of the attack. Was the attack directed at HSE to acquire specific information, or was it random?
- Identify the systems that have been compromised.
- Identify the files that have been accessed and determine the sensitivity of those files.
- Determine whether unauthorized hardware has been attached to the network or whether there are any signs of unauthorized access through the compromise of physical security controls.
- Examine key groups (domain administrators, administrators, and so on) for unauthorized entries. Use tools like "Change Notifier" for Active Directory to detect unauthorized changes to the Active Directory domain accounts.
- Search for security assessment or exploitation software. Cracking utilities are often found on compromised systems during evidence gathering.
- Look for unauthorized processes or applications currently running or set to run using the startup folders or registry entries.
- Search for gaps in, or the absence of, system logs.
- Review intrusion detection system logs for signs of intrusion, which systems might have been affected, methods of attack, time and length of attack, and the overall extent of potential damage.
- Examine other log files for unusual connections; security audit failures; unusual security audit successes; failed logon attempts; attempts to log on to default accounts; activity during nonworking hours; file, directory, and share permission changes; and elevated or changed user permissions.
- Compare systems to previously conducted file/system integrity checks. This will enable identifying additions, deletions, modifications, and permission and control modifications to the file systems or security logs.

5. Recovery

During this phase, the primary objective is to restore the system to its normal operation. The extent of the security breach will determine the approach to system recovery. In collaboration with the Director of IT, the IT team will assess whether the existing system can be restored or if it is necessary to rebuild the affected system entirely.

6. Post-Incident Follow-Up

Following the documentation and recovery phases, the IRT will conduct a comprehensive review of the process. This review will highlight successful execution and areas where errors occurred. It will identify processes that require modification and inclusion in the Response Plan.

6. SEVERITY RATING CATEGORY [1]

For the purpose of this plan, a cybersecurity incident is defined as an event perceived or proven to be an attack on the security of HSE's computing systems. These events may include viruses, phishing, or other attacks initiated by external parties to gain unauthorized access to HSE's data, systems, or other business records. To streamline the response process, the Head of ITIS will assign one of the four severity ratings to reported incidents.

Severity	Symptoms	Action
Reportable (1)	• Minimal impact to small segment of user population; completely localized, with few individuals affected; presenting little or no risk to other entities. • No loss or compromise of sensitive data. • An isolated cybersecurity attack that can be handled by compensating controls. (Examples include a cybersecurity attack that resulted in a single event with no data loss/business compromise; Phishing, virus to a local machine; all incidents that will not affect operation of business.)	• Remedial action. • Notification of IT management
Minor (2)	• Some adverse impact to business • Impact is localized or contained, or minimal risk of propagation. • No apparent release or compromise of sensitive data. (Example: Any security incident which has been successfully responded to and which does not have the potential, over time, to affect inherent operational or reputational risk.)	• Remedial action. • Notification of IT management • Report to the IRT in writing
Major (3)	• Penetration or denial of service attacks attempted with limited impact on operations or larger widespread instances of a new cybersecurity attack not handled by compensating controls or training. • Event that adversely impacts a non-critical HSE system or service • A cybersecurity attack that results in financial loss or public reputational damage	• Remedial action. • Notification to ITIS • Report Incident to Cybersecurity Leadership • Report to the IRT in writing • Log in FBI incident database

Critical (4)	• Successful penetration or denial of service attacks detected with significant impact on operations. • Significant risk of negative financial or public relations impact may result. • Any incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of more than 12 to 48 hours. (Examples include a cybersecurity attack as notified by the FBI or some other law enforcement agency, a cybersecurity risk that exposes confidential data to the public, or a cybersecurity risk that becomes public knowledge	• Invoke Business Continuity Plan (BCP) if all services are down. • Remedial and containment action. • Notification to IT IS • Report Incident to Cybersecurity Leadership • Notify authorities (i.e., FBI and local police) • Document incident and report to the IRT in writing

7. REFERENCES & CITATIONS

[1][2][3][4][5][6] (captured Appendices A-E from Incident response plan template. (n.d.). https://primacentral.org/wp-content/uploads/2023/05/Incident-Response-Plan-Template.pdf)

APPENDIX A - PRIMARY EMERGENCY CONTACT LIST [2]

Department	Primary Contact
Information Technology & Information Security	ITIS@hse.ie
Incident Response Team (IRT)	security-IRT@hse.ie
Applications Development	AD-team@hse.ie
Applications Support	AS-team@hse.ie
Network and Telecommunications	NetTelCom@hse.ie
Systems and Databases	SysDBA@hse.ie
Technical Support	Tech-support@hse.ie
FBI Internet Crime Complaint Center	https://www.ic3.gov

APPENDIX B – INCIDENT RESPONSE PROCEDURE [3]

i. Incidence Discovery Phase

a. The IT staff member or affected department staff member who discovers the incident will contact the Head of ITIS immediately to report the incident.
b. The staff member should include the following information:
    i. Is the equipment affected business critical?
    ii. What is the severity of the potential impact?
    iii. Name of the system or person being targeted, along with the operating system, IP address and physical location.
    iv. IP address and any information about the origin of the attack.

ii. IRT Notification Phase

a. The Emergency Contact List is used to contact the Incident Response Team (IRT).

iii. Analysis and Assessment Phase (Incident Review)

a. The Director of IT / Head of ITIS will review the Incident Response Handling Procedure Flowchart (Appendix C) and determine if the incident is Reportable, Minor, Major or Critical.
b. The following items will be considered when determining the incident severity:
    i. Is the incident real or perceived?
    ii. Is the incident still in progress?
    iii. What data or property is threatened and how critical is it?
    iv. What is the impact on the agency if the attack succeeds? (Minimal, serious or critical?)
    v. What system or systems are targeted and where are they located on the network?
    vi. Is the incident inside the trusted network, outside, or in the DMZ?
    vii. Is the response urgent?
    viii. Will the response alert the attacker? Do we care?
    ix. What type of incident is this (virus, worm, intrusion, abuse, damage, etc.?)
c. Categorize the incident:
    i. Reportable – Disruption to a single person with minimal risk
    ii. Minor – Localized or minimal security risk without threat of compromised data
    iii. Major – Threat to sensitive data
    iv. Critical – Threat to critical systems or entire infrastructure possibly requiring implementation of the Business Continuity Plan.
d. If the incident is major or critical, the Incident Response Team will meet in person or discuss the situation over the phone. The Incident Assessment Checklist will be completed to help determine a response strategy.

iv. Containment Phase

a. Containment action may require the following:

i.) Disconnection of the affected system(s)

ii.) Password changes

iii.) Block ports or connections from external IP addresses

v. Incident Remediation and Response Phase

a. The IRT will establish and follow one or more of the below procedures based on determination after completing the checklist. The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure the team must document what was done and later establish a procedure for the incident.
    i. Worm/Virus/Spyware response procedure
    ii. Active/Inactive intrusion response procedure
    iii. System abuse procedure
    iv. System failure procedure
    v. Property theft response procedure
    vi. Website, Database or Network DOS response procedure
    vii. Event Log Review Procedure

b. IRT members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence. Authorized personnel may vary by situation.

c. Team members will recommend changes to prevent the occurrence from re- occurring or infecting other systems.

d. Upon the approval of the Director of IT (and, if necessary, the Head of ITIS (Information Technology & Information Security) or Cybersecurity Leadership), the changes will be implemented.

vi. Notification Phase

a. Notify affected users

b. Notify Head of ITIS (Information Technology & Information Security)

c. Notify Cybersecurity Leadership members and Superintendent if Major or Critical incident

d. Notify external affected stakeholders if a data breach has occurred.

e. Notify proper external agencies (police, FBI or other appropriate agencies).

f. May be completed before or after System Restoration Phase (or both).

vii. System Restoration Phase

a. Team members will restore the affected system(s) to an "un-affected" state. They may do one or more of the following:
    i. Re-install the affected system(s) from scratch and restore data from backups. Preserve evidence before doing this. Save a copy of the server as evidence if possible.

ii. Require users to change passwords if they have been compromised.
iii. Ensure the system has been hardened by shutting off or uninstalling unused services or features.
iv. Ensure the system is fully patched and protected.
v. Ensure the virus protection is running.
vi. Ensure the system is logging events correctly and at the proper levels.

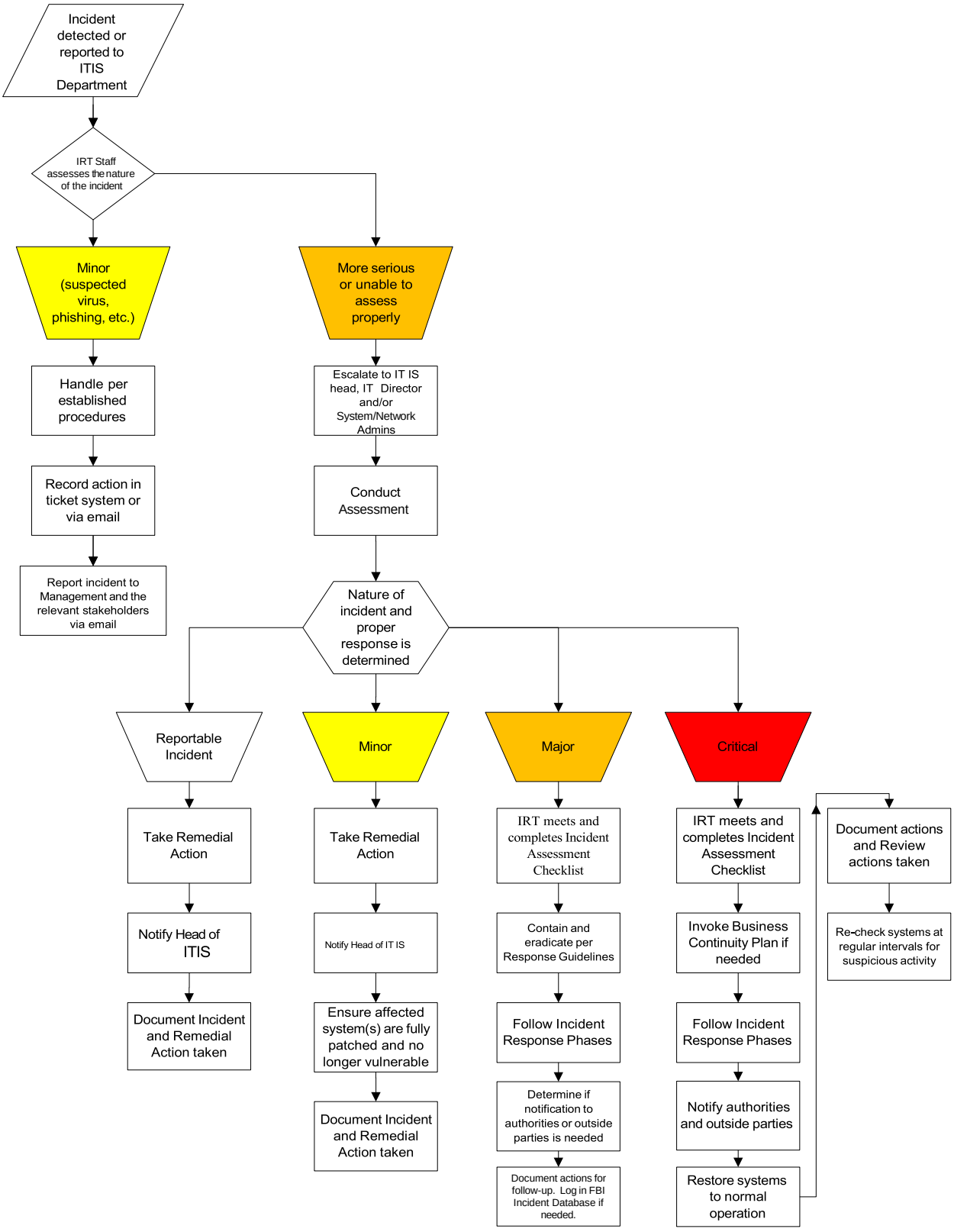
viii. Documentation Phase

a. The following documentation will be kept by using the Incident Assessment Checklist:
   i. How the incident was discovered.
   ii. Severity Rating Category of the incident (Reportable, Minor, Major, Critical)
   iii. How the incident occurred (email, firewall, etc.)
   iv. Where the attack came from (IP address, physical address, other related info)
   v. What the response plan was.
   vi. What was done in response.
   vii. Whether the response was effective.
   viii. Recommendations for procedure improvement.
b. Evidence Preservation – make copies of logs, email, other evidence. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution.

ix. Assessment and Review Response Phase

a. Assess damage and cost to organization and cost of containment efforts.
b. Review response and update policies
   i. Consider whether an additional policy could have prevented the intrusion. Should any security policies be updated?
   ii. Consider whether a procedure or policy was not followed which allowed the intrusion. Consider what could be changed to ensure the procedure or policy is followed in the future.
   iii. Was the incident response appropriate? Could it be improved?
   iv. Were the incident response procedures detailed and did they cover the entire situation? Can they be improved?
   v. Was every appropriate party informed in a timely manner?
   vi. Could changes be made to prevent re-infection? Have all systems been fully patched, locked down, passwords changed, antivirus updated, etc.?
   vii. What lessons have been learned from this experience?

Appendix C - Incident Response Procedure Flowchart [4]



Appendix D - Incident Assessment Checklist [5]

The activities described in this checklist are designed to assist in the initial assessment process performed and/or conducted by the Incident Commander (IC), as specified in [HSE-IR-POL-2024]

Completion of this checklist is essential for any incident that calls for the execution of the Information Security Incident Response Protocol. Once the Incident Response Team is assembled, the Assessment Checklist is reviewed for completion to ensure all pertinent facts are established.

A. Description of Incident - Data relevant to the Incident should be collected for use in the process of Incident determination.
A1. Record the current date and time.
A2. Provide a brief description of the Incident.
A3. Who discovered the Incident? Provide name and contact information.
A4. Indicate when the incident occurred and when it was discovered.
A5. How was the Incident discovered?
A6. Describe the evidence that substantiates or corroborates the Incident (e.g., eye-witness, time- stamped logs, screenshots, video footage, hardcopy, etc.).

A7. Identify all known parties with knowledge of the Incident as of current date and time.
A8. Have all parties with knowledge of the Incident been informed to treat information about the Incident as "sensitive or confidential"?
B. Types of Information, Systems and Media - Provide information on the nature of the data that is relevant to the Incident.
B1. Provide details on the nature of the data (e.g., email, agency data, client data, etc.).
B2. Does the information (if compromised) constitute a violation of regulatory requirements or HSE's policies? Describe what is known.
B3. Was the compromised information maintained by HSE or a 3rd Party (i.e., outside agency, etc.)? Provide details.
B4. How was the information held? Identify the types of information systems and/or the media on which the information was stored (e.g., server, laptop, USB drive, etc.).

B5. If the information was held electronically, was the data encrypted or otherwise disguised or protected (e.g., redacted, partial strings, password required, etc.)? If so, describe measures taken.
B6. What steps are required or being taken to preserve evidence of the Incident? Describe.
C. Risk/Exposure - Attempt to determine to what extent risk and/or exposure is presented by this Incident.
C1. Can we reasonably determine the risk or exposure?
C2. To what degree are we certain that the data has or has not been released?
C3. Do we have contact with someone who has "firsthand" knowledge of the circumstance (e.g., the owner of a stolen device, laptop, etc.)? Provide name and contact information.
C4. What firsthand knowledge have we determined? Describe what is known.
C5. Can we identify and do we have contact with the party that received the data or caused the compromise? Describe what is known.
C6. Identify the impacted parties, if possible.

C7. What is the risk or exposure to HSE? Describe.
C8. What is the risk or exposure to the Client? Describe.
C9. Can we determine to what extent news outlets may know of this Incident? Describe.
D. Next Steps - Determine what information or action is required to better assess or address this Incident.
D1. Do we have enough information to establish the category and severity of the Incident? - If "yes", declare the Incident category and severity. - If "no", describe what else might be required.
D2. If additional data collection data is required, assign responsibility to IRT member for collection and reporting to IRT.
D3. Is there any deadline or reporting requirement (self-imposed or regulatory) we need to address?
D4. What communications need to be established?
D5. Are there any immediate issues that have not been addressed? Describe.

E. Documentation – Document the incident and determine preventative steps so the incident can be avoided in the future.
E1. What steps were taken to address the incident? What response plan was followed?
E2. Was the response plan effective? If so, why?
E3. How could the response plan be improved?
E5. Have changes been made to prevent a re-occurrence of the incident or re-infection? Have all the systems been patched, locked down, etc.?
E6. Should any security policies be updated?
E7. What did we learn from this experience?

Appendix E - Technical Controls [6]

i. Virus Protection

- Trend Micro Deep Security for servers in the virtual infrastructure
- Trend Micro Deep Security for virtual desktops in the virtual infrastructure
- Sophos Antivirus for desktops and laptops
- Both systems are configured for on-line scanning
- Weekly scans for Sophos
- Daily virus definition updates
- Malicious activity alert notifications are sent to the IT Service Desk for investigation.
- Antivirus detection on Internet connection through Palo Alto firewall

ii. Spam Filtering

- Microsoft Office 365 for filtering incoming SPAM email messages
- Barracuda Anti-Spam server for filtering list server SPAM

iii. Content Filtering

- Lightspeed Systems used for Web filtering and activity reporting
- Palo Alto firewalls used to monitor all Internet activity
- Access controls and policies are used to control Internet traffic.
- Content filters are used to block pornographic, inappropriate and malicious websites.

iv. Spyware screening

- Palo Alto Networks Spyware prevention
- Sophos anti-virus and Malwarebytes

v. Intrusion Prevention System

- Palo Alto firewalls

vi. Periodic User Alerts

- The ITIS Department sends out periodic alerts to all HSE employees, alerting them about potential phishing, malware or other security exploits that may be received via electronic mail.
- Employees are reminded to never click on any links included in email messages and always double check with a tech support staff if a message appears suspicious but may be work related. Otherwise, they should delete the email message.

Appendix F: Linkage to other relevant documents

The policy uses terms, abbreviations and cross-references which are liaised in the [HSE-IR-POL-2024] and [HSE-PLYBOOK-001] documents. Following are the attached copies of the documents prepared by the consultant.

[HSE-PLYBOOK-001]	HSE Ransomware Playbook v0.1.pdf
[HSE-IR-POL-2024]	HSE Incident Response Policy v0.1.