



Information and Communication Incident Management Plan





DIRECTORATE: OFFICE OF THE CEO	
SUBJECT: ICT INCIDENT MANAGEMENT PLAN	NO:
REV NO: 1	REV DATE: 10 May 2023
SUB-DIRECTORATE: Information Management	BOARD ITEM NO:
SIGNATURE:	
DATE APPROVED:	EFFECTIVE DATE: 01 July 2023

1. INTRODUCTION

Incidents may be established by reviewing a variety of sources including, but not limited to ITSO monitoring systems, reports from service providers' staff or outside organisations and service degradations or outages. Discovered incidents will be declared and documented in ITSO's incident documentation system.

Complete IT service outages may also be caused by security related incidents, but service outage procedures will be in detail in business continuity plan and/or disaster recovery procedures.

Incidents will be categorized according to potential for restricted data exposure or criticality or resource using a **High---Medium---Low** designation. The initial severity rating may be adjusted during plan execution. This will determine the magnitude and the weakness of the security incident to make decisions. Response plan is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

Detected vulnerabilities will not be classified as incidents. The ITSO deploys tools to scan the environment and depending on severity of found vulnerabilities may warn affected users, disconnect affected machines, or apply other mitigations. In the absence of indications of sensitive data exposure, vulnerabilities will be communicated and the ITSO will pursue available technology remedies to reduce that risk.

2. PURPOSE

The Incident management plan document describes the overall plan for responding to information security incidents at CENTLEC. It defines the roles and responsibilities of

participants, characterisation of incidents, relationships to other policies and procedures, and reporting requirements. The goal of the computer security Incident

3. SCOPE

This plan applies to the information systems, organisational data, and networks of CENTLEC and any person or device that gains access to these systems or data.

4. ABBREVIATIONS

4.1	ITSO	–	Information Technology Security Officer
4.2	CIO	–	Chief Information Officer
4.3	CSO	–	Chief Security Officer
4.4	IT	–	Information technology
4.5	PHI	-	Protected Health Information
4.6	ICT	–	Information and Communication technology
4.7	MMM	–	Mangaung Metro Municipality
4.8	PHI	–	Protected Health Information
4.9	SOP	–	Standard Operational Procedure
4.10	PII	-	Personal Identification Information

5. RELATED DOCUMENTS

This policy relate to standard operating procedure that deals with incident management procedure, backup procedure and change control procedure, physical , environmental policy , ict security policy and CENTLEC security management policy. This plan incorporates the risk profiles for Institutional data as outlined in the guidelines for data classification method e.g. classified, and confidential.

6. DEFINITIONS

- 6.1 **Event** – an event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

- 6.2 **Information technology security officers** - monitor the organisation's IT system to look for threats to security, establish protocols for identifying and neutralizing threats, and maintain updated anti-virus software to block threats
- 6.3 **Chief information technology security officer** - is a person responsible for the safety and security of company data, personnel, and assets. One key responsibility of the CITSO is preventing data breaches, phishing, and malware, by developing robust safety protocols and crisis management.
- 6.4 **The Health and Safety Officer** - is responsible for tasks such as: Developing, implementing, and improving the health and safety plans, programmes and procedures in the workplace. Ensuring compliance with relevant health and safety legislation. Identifying OHS-related training needs in the workplace.
- 6.5 **Risk officer** – is a person managing all risk function aspects in a business. Identifying, measuring, managing and reporting risks. Helping develop processes to better evaluate business-specific risk. Monitoring important as well as critical risk issues.
- 6.6 **Information technology** - is building communications networks for a company, safeguarding data and information, creating and administering databases, helping employees troubleshoot problems with their computers or mobile devices, or doing a range of other work to ensure the efficiency and security of business information.
- 6.7 **Chief information officer (CIO)** - is the company executive responsible (Currently is the executive manager retail in absence of CIO), for the management implementation, and usability of information and computer technologies. Because technology is increasing and reshaping industries globally, the role of the CIO has increased in popularity and importance.

- 6.8 **Incident Response Coordinator** - coordinates the process of reporting incidents by: Encouraging person(s) affected to report the occurrence to Public Safety for investigation and/or prosecution.
- 6.9 **Incident** - incident is an event that, as assessed by ITSO staff, violates the Information Security Policy; other CENTLEC policy, standard, or code of conduct, or threatens the confidentiality, integrity, or availability of information systems or institutional data.

7. PERSONALLY IDENTIFIABLE INFORMATION

For adhering to security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements to identify personal bridges

- 7.1 Identity number card number
- 7.2 driver's license number

8. ROLES AND RESPONSIBILITIES

The Incident Response Process incorporates the Information Security Roles and Responsibilities definitions and extends or adds the following Roles.

8.1 **Incident response coordinator**

The Incident Response Coordinator is the ITSO within ICT who is 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.

8.2 **Incident response handlers**

Incident Response Handlers are employees in ICT working closely with

ITSO, other CENTLEC staff, or outside contractors who gather, reserve and analyses evidence so that an incident can be brought to a conclusion.

8.3 **Insider threats**

Insiders are current or former employees, contractors, or business partners who has an access to an organization's restricted data and may use their access to threaten the confidentiality, integrity or availability of an organisation's information or systems. This particular threat defined because it requires the enforcement of the user access management policy and procedure to ensure that users who left the organisations is deactivated immediately from the systems with the notification from human resource department as defined in the ict user access management policy and procedure.

8.4 **CENTLEC Security Officers**

Security officers are the staff designated for various regulatory framework to which CENTLEC is required to comply. ITSO staff will escalate the incident offence where incident involves criminal activities to the security manager as per CENTLEC security management policy.

8.5 **Users**

Users are employees of the CENTLEC or anyone accessing information system, organisational data or CENTLEC networks whom the incident might affect. These users should report the incident to servicedesk as per incident management procedure.

8.6 **Maintenance team**

The CENTLEC information security officer (ITSO) is responsible for the maintenance and revision of this document.

8.7 **ITSO**

The ITSO is in charge with executing this plan by virtue of incident investigation and reporting according various policies such as the internet policy, ict security policy, firewall policy, user access management policy and change control policy.

8.8 **CENTLEC GROUPS**

The ITSO acts on behalf of the CENTLEC client and will ask for cooperation and assistance from auditors as required. The ITSO also works closely with CENTLEC administrative groups such as the auditors, human resources, and office of the chief security in investigations unit.

9. **METHODOLOGY**

9.1 This plan outlines the most general tasks for incident response and will be supplemented by specific internal guidelines and procedures that describe the use of security tools and/or channels of communication.

These internal guidelines and procedures are subject to amendment as technology changes. It is assumed that these guidelines will be documented in detail and kept up to date.

The ITSO represents the entire CENTLEC information system(s) and institutional data, supporting the Users. ITSO will attempt to coordinate its efforts with these other groups and to represent the CENTLEC'S security posture and activities.

9.2 **Evidence Preservation**

The goal of Incident Response is to reduce and contain the scope of an incident and ensure that IT assets are returned to service as quickly as possible. Rapid response is balanced by the requirement to collect and preserve evidence in a manner consistent with the requirements. ITSO

will maintain and disseminate procedures to clarify specific activities in the ITSO and in CENTLEC departments with regard to evidence preservation, and will adjust those procedures as technologies change.

9.3 Operational Level Agreements, and Governance

Interruption of service is a hardship and the ITSO will cooperate with these groups to ensure that downtime is minimised. However, the ITSO's management supports the priority of investigation activities where there is significant risk, and this may result in temporary outages or interruptions.

9.4 Staffing for an Incident Response Capability, Resiliency

The ITSO will endeavor to maintain sufficient staffing and third party augmentation to investigate each incident to completion and communicate its status to other parties while it monitors the tools that detect new events. Insufficient staffing will affect rapid response capability and resiliency, as will degradation of the tools used for detection, monitoring and response.

9.5 Training for incident

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested and translated into recommendations for enhancements. CENTLEC employees inside and ITSO will be periodically trained on procedures for reporting handling incidents to ensure that there is a consistent and appropriate response to incidents, and that post incident findings are incorporated into procedural enhancements. This incident are information security event, e.g. noting all details immediately, such as type of non-compliance or breach using email fishing for users, or continuous suspicious messages on the screen. This should immediately reported to the CENTLEC servicedeks as the point of contact.

10. INCIDENT RESPONSE PHASES

The basic incident process encompasses six phases: preparation, detection, containment, investigation remediation and recovery. The ITSO's overall incident response process includes detection, containment, investigation, remediation and recovery, documented in specific procedures it maintains. This plan is the primary guide to the preparation phase from a governance perspective; local guidelines and procedures will allow the ITSO to be ready to respond to any incident. Recovery includes reevaluating whether the preparation or specific procedures used in each phase are appropriate and modifying them if inappropriate.

10.1 Incident preparation

Preparation includes those activities that enable the ITSO to respond to an incident policies, tools, procedures, effective governance and communication plans. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post analyses from prior incidents should form the basis for continuous improvement of this stage.

10.2 Incident Detection

Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident.

10.3 Incident Containment

Containment is the triage phase where the affected host or system is identified, otherwise mitigated, and when affected parties are notified and investigative status established.

10.4 Incident Investigation

Investigation is the phase where ITSO personnel determine the

priority, scope, and root cause of the incident. Then escalate the incident for reporting to the manager, executives. This incident will further escalated to the Centlec security officer should it involve any acritical act or need forensic investigation. The security manager will handle the incident as per Centlec security management policy within his/her department

10.5 **Incident remediation**

Remediation is the post incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been contained. The determination of whether there are regulatory requirements for reporting the incident (and to which outside parties) will be made at this stage in cooperation with Office of the CENTLEC security office.

10.6 **Recovery**

Recovery is the analysis of the incident for its procedural gathering of metrics and incorporation of “lessons learned” into future response activities and training. Specific procedures related to this Incident response plan is documented at the plan and procedures.

10.7 **Counters actions**

The disciplinary procedure will be taken by CENTLEC where criminal act or security breaches which led to the incident committed by the internal personnel

11. INCIDENT RESPONSE PROCESS

In the process of responding to an incident, many questions arise and problems encountered, any of which may be different for each incident. This section provides guidelines for addressing common issues. The Incident response coordinator, manager Information management and office of the chief security should be consulted for questions and incident types not covered by these guidelines.

11.1 Insider Threats Analysis

In the case that a particular Incident Response Handler is a person of interest in an incident, the Incident Response Coordinator will assign their incident response handlers to the incident.

In the case that the Incident response coordinator is a person of interest in an incident, the executive manager on behalf of CIO will act in their stead or appoint a designee to act on their behalf. In the case that the manager information management is a person of interest in an incident, the Chief Executive Officer will act upon the incident handling to make informed decisions. In the case, that another Security officer administrative authority is a person of interest in an incident, the ITSO will work with the remaining administrative authorities in the ITSO is reporting line to designate a particular point of contact or protocol for communications.

11.2 Communications

All public communications about an incident or incident response to external parties outside of CENTLEC are made in consultation with communication department. Private Communications with other affected or interested parties contain the minimum Information necessary. The incident response Coordinator and the Manager of information management determine the minimum information necessary to share for a particular Incident.

Table 1: Communication process

Responsible person	Title	Section	Contacts
Daniel Malokase	Manager	ICT	051 412 2634
Ambeswa Ngetu	Information Technology Security Officer	ICT	051 412 2438

Gerald Nkota	Chief Security Officer	CENTLEC Security	051 409 2207
Hlomlani Dhlamini	Risk Asst Manager	Audit and Risk	051 409 2779
Nico Moeketsi	Manager	Health and Safety	051 409 2360
Lele Mamatu	GM	Communication	051 409 2718

11.3 **Privacy**

The security policy provides specific requirements for maintaining the privacy of CENTLEC affiliates. All incident response procedures will follow the current privacy requirements as set out in the ict security policy and user access management policy.

11.4 **Escalation**

At any time during the incident response process, the Incident response coordinator and the manager information management may be called upon to escalate any issue regarding the process or incident. The Incident response coordinator and manager information management in consultation with chief executive officer will determine if an incident should be escalated to external authorities.

11.5 **Documentation and reporting**

All incidents response activities will be documented to include items obtained using methods consistent with chain of custody and confidentiality requirements. Incidents will be prioritized and ranked according to their potential to disclose restricted data in the incident management document.


This will also be logged in the systems as per incident management procedure and closed with remarks after the incident as per incident management procedure. As an investigation progresses, that ranking may change, resulting in a greater or lesser prioritization of ITSO resources. Incidents will be reviewed to assess whether the investigational process was successful and effective. Subsequent adjustments may be made to

methods and procedures used by the ITSO and by other participants to improve the incident response process according to incident management procedure. In the case where Information technology security officer resigned or not being available for incident analysing and investigation. The executive manager will delegate and authorise the senior personnel to resume the role of the information and technology security officer.

12. REVIEW AND APPROVAL

This Plan and underlying strategies will be review at least annually, or as necessary, to ensure its continued application and relevance.


Revised by:

Signed: 
Manager: Information Management
Date: 22 / 05 / 2023

Supported by:

Signed: 
Act Executive Manager: Engineering Retail
Date: 22 / 05 / 2023

Approved by:

Signed: 
Chief Executive Officer
Date: 22 / 05 / 2023