



Approval Date	28/03/2022
Periodical Review	Annually
Commencement Date	28/03/2022
Review Date	28/03/2023

STANDARD OPERATING PROCEDURE: INCIDENT MANAGEMENT

TITLE OF SOP	Incident Management Procedure
SOP Number	CIO-01
Purpose	The purpose of this procedure is to manage IT service disruptions and ensure the disrupted services are restored within agreed SLA. It will define the processes for notifying management about and responding to information security incidents, as well as cover types of incidents and response strategies and the roles and responsibilities of employees.
Scope	This procedure applies to all employees using ECSDS network and support services.
Definitions and Acronyms	<p>Incident is an unplanned interruption to a service or reduction in a quality of a service.</p> <p>Minor incident is an incident that impacts on a single user or unit.</p> <p>Major Incident is an incident that affect business critical services and require immediate resolution.</p> <p>Service Desk Agent - Help desk agent act as the first point of contact between customers who need technical support and the IT department.</p> <p>ICT – Information and Communication Technology</p> <p>User - Refers to the Departmental official that is requesting ICT service</p> <p>SLA – Service Level Agreement</p> <p>SCM – Supply Chain Management</p>
Performance Indicator	Number of Governance compliance initiatives implemented

STEP BY STEP GUIDE

INCIDENT MANAGEMENT

Nr	Task Name	Task Procedure	Responsibility	Time Frames	Systems and Supporting Documentation	Service Standard
1.	Log the Incident	<ul style="list-style-type: none"> • When an employee suspects an event has occurred, • Contact the ECDSD help desk / submit incident report form, providing as much of the following information as possible: <ul style="list-style-type: none"> ✓ location(s) where the incident(s) occurred; ✓ contact information (this includes: contact name, bureau/office, telephone number, etc.); ✓ date and time of the incident(s); ✓ description of the incident(s); ✓ identification of the computing devices used in the security incident(s) (if known); ✓ name of the person(s) who may have committed the security breach (if known); and ✓ name and work location of witness (if any). • The ECDSD help desk will capture all suspected incidents on the system. 	User	1 Day	<ul style="list-style-type: none"> • System Reference No • Incident Report Form 	Resolve all logged incidents and closed 14 days after resolution provided that the client has not indicated dissatisfaction within the resolution as SLA for SITA services delivered to the Department of 2018 and also as indicated from MS Premier Support Services
2	Categorise the Incident	<ul style="list-style-type: none"> • Establish whether or not an incident has occurred. • Determine whether the incident activity is actively occurring or has ceased; if ceased, whether it is likely to resume. • Determine which and how many systems and data are actually or likely affected. • Assess whether the incident activity has occurred solely within your domain, or whether external activity is involved (as a source or downstream target). • Classify the incident (major, minor) 	Service Desk Agent	1 hour	<ul style="list-style-type: none"> • System Reference No • Incident Report Form • Categorized reported calls 	

3	Provide 1st line Support to resolve the Incident	<ul style="list-style-type: none"> • Attempt to resolve the incident • If unable to resolve, escalate the incident to the appropriate technician who will initiate an investigation 	Service Desk Agent	1 hour	<ul style="list-style-type: none"> • Incident Management System • Resolved Call • Escalated call (where applicable) 	
4	Provide 2nd line Support to resolve the Incident	<ul style="list-style-type: none"> • Perform tasks according to the nature of the incident. In cases where an incident cannot be resolved within IT, escalate to the third party. 	Technician	2 working days	<ul style="list-style-type: none"> • Incident Management System • Escalated call (where applicable) • Resolved Call 	
5	Close the Incident	<ul style="list-style-type: none"> • When the incident has been resolved, get feedback or acknowledgement from the user to check if s/he is satisfied with the resolution. • Close the call after the incident has been resolved. • After the incident has been closed, document all take-aways from the incident. 	Service Desk Agent	1 working days	<ul style="list-style-type: none"> • Incident Management System • Client satisfaction acknowledgement • Closed incident call 	



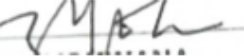

LEGISLATION REFERENCES

Document Name	Document Description
Information Security Policy 2016	Implementation Guideline for Corporate Governance of Information and Communication Technology.
ITIL Version 4 2019	Information Technology Infrastructure Library framework designed to standardise the selection, planning, delivery, maintenance and overall life cycle of IT service within a business. Objective: Incident Management aims to manage the lifecycle of all Incidents (unplanned interruptions or reductions in quality of IT services). The primary objective of this ITIL process is to return the IT service to users as quickly as possible.
COBIT 2019	Control Objectives for Information and related technologies to develop, organise and implement strategies around information management and governance.
Provincial SITA Business Agreement 2019	To establish a contractual relationship between the client (Department) and SITA for provision of information systems, information technology and related services by SITA to the client and to regulate such relationship as intended by SITA act, 1998, as amended, and Regulations thereto.
Department SITA Service Level Agreement 2018	To establish the level of service delivery between the client (Department) and SITA, acting as the service provider, for the rendering of SITA services.
Microsoft Services Premier Support	Comprehensive solution to support the Department of Social Development in improving and maintaining the health of your Microsoft platform infrastructure.

RISKS

Risk Name	Risk Description	Probability (H/M/L)	Impact (H / M / L)	Control Description	System / Manual
Unavailability of the user	<ul style="list-style-type: none"> User unavailability lead to the delay in resolving the call. 	M	H	<ul style="list-style-type: none"> Inform the user prior the visit to resolve the call 	Manual
	<ul style="list-style-type: none"> Business continuity can also be affected. 	L	H		
Insufficient Resources	<ul style="list-style-type: none"> When the work is more that the human resource available to perform the task this can lead to burnout. Unavailability of Transport and Accommodation Budget. 	H	H	<ul style="list-style-type: none"> Use of Interns Use of Service Portal Dedicated vehicle for ICT Operations 	Manual

AUTHORIZATION

Designation:	Name:	Comment:	Signature:	Date:
Recommended By: Director-ICT Engineering	T.M. Vazi			18/03/2022
Recommended by: Acting CIO	M.E. Gazi	Aligned with reviewed ICT policies		18/3/2022
Recommended by: DDG	N.Z.G Yokwana	Recommended		24/03/2022
Approved by: Head of the Department	M. Machemba	Approved		28/03/2022
Distribution and Use of SOP	All CIO Directors, All CIO Deputy Directors, All CIO Assistant Directors, All CIO Administration support staff, All CIO Personal Assistance			