



Province of the  
**EASTERN CAPE**  
COOPERATIVE GOVERNANCE  
& TRADITIONAL AFFAIRS

---

## **ICT INCIDENT RESPONSE POLICY**

<b>Departmental Contact Details</b>	
<b>Physical Address</b>	<b>Tyamzashe Building Phalo Avenue Bhisho 5605</b>
<b>Postal Address</b>	<b>Department of Cooperative Governance and Traditional Affairs Private Bag X0035 Bhisho 5605</b>
<b>Document Number</b>	<b>2</b>
<b>Document Name</b>	<b>ICT Incident response Policy</b>
<b>Custodian</b>	<b>Ms T.M. Luke</b>
<b>Designation</b>	<b>Director: Information Management Services</b>
<b>Component</b>	<b>DGITO</b>
<b>Telephone No.</b>	<b>040 940 7235</b>
<b>Cell Phone No.</b>	<b>076 141 1749</b>
<b>E-mail Address</b>	<b><a href="mailto:tswakai.luke@eccogta.gov.za">tswakai.luke@eccogta.gov.za</a></b>
<b>Date Completed</b>	<b>April 2022</b>
<b>Date of Approval</b>	
<b>Date Last Amended</b>	<b>31 January 2017</b>
<b>Date For Next Review</b>	<b>April 2027</b>
<b>Related Policies</b>	<b>Internet and Email Use Policy</b>


**SIGN OFF**

**Head of Department**

This Policy has been recommended by Mr. AA Fani in my capacity as Head of Department of Department Cooperative Governance and Traditional Affairs.

I am satisfied and concur with the contents of this Policy.


The development of the policy on ICT Incident Response will ensure the department is able to exercise its powers in compliance with the law and guide decision making in the department.

<b>Signed</b>	
<b>Designation</b>	Mr. A.A Fani, Head of Department: Cooperative Governance and Traditional Affairs
<b>Date</b>	13/09/2022

**Executive Authority**

The Department of Cooperative Governance and Traditional Affairs has an unprecedented opportunity to improve the livelihoods of the people by effectively rendering the many services that it is expected to provide. We have envisaged a department that has the required capacity to respond adequately to challenges of its people.

I therefore trust that guidance from this ICT Incident Response Policy will contribute to the effective utilization of the policy by the staff of the department.

<b>Signed</b>	
<b>Designation</b>	MEC: Honourable Z Williams of Cooperative Governance and Traditional Affairs
<b>Date</b>	19/09/2022.

**1. CONTENTS**

1. PREAMBLE ..... 5

2. PURPOSE OF POLICY ..... 5

3. POLICY OBJECTIVES..... 5

4. DEFINITIONS ..... 5

5. APPLICATION AND SCOPE ..... 6

6. LEGISLATIVE FRAMEWORK..... 6

7. CONSULTATION PROCESS WITH STAKEHOLDERS ..... 6

8. POLICY PRINCIPLES INHERENT IN THE ICT ACCEPTABLE USE POLICY ..... 6

9. POLICY STATEMENT ..... 7

10. POLICY CONTENT ..... 7

10.1. INCIDENT DETECTION AND ASSESSMENT ..... 7

10.2. INCIDENT CLASSIFICATION..... 8

10.3. COMMUNICATION AND ESCALATION ..... 8

10.4. INCIDENT RESOLUTION..... 8

10.5. INCIDENT POST RESOLUTION ..... 8

10.6. RECORDING OF INCIDENTS AND FOLLOW UP ..... 9

11. ENFORCEMENT PROCEDURES ..... 9

12. MONITORING AND EVALUATION OF THE IMPLEMENTATION OF THE POLICY .. 9

13. COMMUNICATION / EDUCATION OF THE POLICY ..... 9

14. DISPUTE RESOLUTION MECHANISM ..... 10

15. APPROVAL OF THE POLICY ..... 10

16. REVIEW OF THE POLICY ..... 10

17. VERSION CONTROL AND CHANGE HISTORY ..... 11

**1. PREAMBLE**

Ensuring the **confidentiality, integrity, and availability** of information assets, information systems and the networks that deliver the information is of outmost importance to any organisation. The Department of Cooperative Governance and Traditional Affairs is committed to implementing all necessary measures to control, mitigate or contain all incidences that occur in its ICT environment to avoid compromise of data.

**2. PURPOSE OF POLICY**

The purpose of this policy is to establish a protocol to guide responses to a computer incident or event impacting the Department’s computing systems.

**3. POLICY OBJECTIVES**

To enable prompt and effective reporting of, and response to all forms of security incidents, be they information, physical, technical or theft, thereby enabling prompt and effective management of the incidents.

**4. DEFINITIONS**

<b>Word/Terminology</b>	<b>Definitions (with examples if required)</b>
COGTA/ the Department	Department of Cooperative Governance and Traditional Affairs
DGITO	Departmental Government Information Technology Office
ICT	Information Communication Technology
Incident	An Incident is defined as an unplanned interruption or reduction in quality of an IT service
DGITO Helpdesk Officer	A person who provides first level support to all departmental users

**5. APPLICATION AND SCOPE**

This policy is applicable to the following employees of the department of Cooperative Governance and Traditional Affairs: -

- (a) Those employees who are employed in terms of the Public Service Act, 1994,
- (b) Those employees who are employed in terms of the Ministerial Handbook,
- (c) Those who are deemed Public Office Bearers and
- (d) any person employed by the department in a temporary or contractual capacity

**6. LEGISLATIVE FRAMEWORK**

The following publications govern the execution of the ICT Incident Response Policy and were taken into consideration during the drafting of the guidelines and policy:

- I. State Information Technology Act (Act no 88 of 1998);
- II. Protection of Information Act (Act no 84 of 1982);
- III. Minimum Information Security Standards (MISS),
- IV. DPSA Corporate Governance of ICT Policy Framework 2012;
- V. Departmental Internet and Email Policy;
- VI. Departmental ICT Security Policy;
- VII. Departmental ICT Acceptable Usage Policy

**7. CONSULTATION PROCESS WITH STAKEHOLDERS**

The Departmental Senior Management Service members have been consulted for inputs during the review of this policy.

**8. POLICY PRINCIPLES INHERENT IN THE ICT ACCEPTABLE USE POLICY**

**I. TRANSPARENCY**

This policy will be made available to all categories of employees within the Department.

## II. PARTICIPATION

All relevant stakeholders will be required to adhere to the content of this policy.

## III. ACCOUNTABILITY

Everyone who has been entrusted with an ICT asset or resource will be required to account for non-adherence to the provisions of this policy.

## 9. POLICY STATEMENT

The Department has a legislative mandate to develop, implement and maintain systems and procedures that ensure an appropriate response to any actual or suspected security incidents relating to information assets, information systems and the networks.

## 10. POLICY CONTENT

### 10.1. INCIDENT DETECTION AND ASSESSMENT

Three types of information sources feed information regarding the incident:

- I. Based on knowledge and training the **End-users** can detect a suspicious activity that has a potential of resulting in a serious ICT security incident.
- II. Operational Personnel (DGITO technical staff) detects incidents in the infrastructure which could provide service disruption which could be experienced by the end user.
- III. Management Systems (Automated System) monitor and detect incidents automatically triggering alerts based on system thresholds and failures.

To report identified information technology incident or situation of potential concern, computer users must use the following contacts to report the following numbers:

- IT Helpdesk at (040) 940-7242/7442
- Email: [dgito@eccogta.gov.za](mailto:dgito@eccogta.gov.za)

DGITO technical staff after receiving a report will capture the incident on the Helpdesk System and allocate it to the appropriate support technician for the incident in question and in cases of extreme severity or time-sensitivity, may also provide a preliminary notification to the GITO.

Upon consideration and assessment of an event notification, the GITO or nominee may declare a formal ICT incident. An event will be considered an incident only upon such declaration.

### **10.2. INCIDENT CLASSIFICATION**

Incidents must be classified to determine priority level to ensure appropriate action by invoking the right technical support at the right time.

Incidents must be classified according to High, Medium and Low priority.

### **10.3. COMMUNICATION AND ESCALATION**

The communication and escalation processes will be conducted with the aim to ensure that all relevant parties are informed of the incident and that status updates are communicated.

Incidents with Critical and High Priority must be communicated to the ICT Security Manager and Members of the Senior Management Service of the Department due its high level of impact. For incidents with Low and Medium Priority, the affected users must be kept updated of progress towards resolving the incident.

### **10.4. INCIDENT RESOLUTION**

During this phase, technical investigations will take place in order to bring the incident into resolution. Personnel from various technical and non-technical business areas may be required in order to provide effective resolution.

### **10.5. INCIDENT POST RESOLUTION**

The post resolution process is initiated once the incident has been resolved.



Critical Incident Review – DGITO to hold Incident Review meetings within 3 working days of the incident resolution. This is attended by all key support staff involved in the incident.

Critical Incident Report – The output of the Critical Incident Review meeting is the Critical Incident Report. This summarises the events of the incident, the impact, actions taken to resolve the incident and further actions being taken to mitigate the risk of future occurrence/impact.

All incidents, critical and non-critical, shall be reported to the ICT Steering Committee on a quarterly basis.

#### **10.6. RECORDING OF INCIDENTS AND FOLLOW UP**

DGITO shall maintain a central register of all incidents occurring and affecting the Department. If there is no reduction in the volume of each type of incident, the ICT Steering Committees will be alerted by the GITO with recommendations for appropriate action to be taken.

#### **11. ENFORCEMENT PROCEDURES**

- Implementation of group policies

#### **12. MONITORING AND EVALUATION OF THE IMPLEMENTATION OF THE POLICY**

DGITO will report any challenges that arise in the implementation of this policy to the ICT Steering Committee.

#### **13. COMMUNICATION / EDUCATION OF THE POLICY**

The Policy will be communicated to Departmental employees through induction workshops / policy rollout sessions, internal news bulletin and be made available on the departmental intranet for sharing information.

**14. DISPUTE RESOLUTION MECHANISM**

In the event of disputes arising out of this policy, such disputes will be dealt with in terms of the grievance procedure and labour legislation applicable in the Public Service.

**15. APPROVAL OF THE POLICY**

The policy will be approved by Member of Executive Council (MEC) on the recommendation of the Head of Department.

**16. REVIEW OF THE POLICY**

This policy will be reviewed on every fifth year from the date of approval and/or when there are changes in legislation or the operating environment.

**17. VERSION CONTROL AND CHANGE HISTORY**

Version Control	Date Effective	Approved By	Amendment
Start from	YYMMDD (The date the policy takes effect)	Contact person – full name & title.	Include any superseded procedures and what the amendment is to the document.
2013		Mlibo Qhoboshiyane (MEC)	
2016		F.D. Xasa	Date driven review
2022		Honourable Z Williams (MEC)	Date driven review