DETERMINATION AND DIRECTIVE ON ICT SERVICE CONTINUITY IN THE PUBLIC SERVICE

TABLE OF CONTENTS

1. INTRODUCTION

1.1. The effect of the current pandemic has had unimaginable disruption on organizations and businesses globally.

1.2. In addition to disruption, the pandemic also presented numerous lessons upon which all stakeholders, including the public service, can learn. For instance, arrangements for alternative workspaces in disruptions proved inadequate as all organizations were affected. This included organizations whose business is the provision of alternative workspaces during disruptions as such environments had to close as well.

1.3. Organizations that were ill-prepared for the business disruption were impacted more adversely than those with concrete and implementable plans for continuity of their businesses during disruptions, even within a single sector.

1.4. Business Continuity Management System (BCMS) emphasizes the importance of understanding the organization's needs and the necessity for establishing business continuity management policy and objectives, implementing and operating controls and measures for managing an organization′s overall capability to manage disruptive incidents, monitoring and reviewing the performance and effectiveness of the BCMS, and continual improvement based on objective measurement (ISO 22301; 2012).

1.5. A BCMS consists of the following components:

a) Business Management Policy (inclusive of ICT Service Continuity Issues);
b) people with defined responsibilities;
c) management processes relating to
    1) policy,
    2) planning,
    3) implementation and operation,
    4) performance assessment,
    5) management review; and
    6) improvement;
d) documentation providing auditable evidence; and
e) any business continuity management processes relevant to the organization (ISO 22301; 2012).

1.6. Business Continuity Management (BCM), as part of the BCMS, is an integral part of a holistic risk management process that safeguards the interests of an organization's key stakeholders, reputation, brand, and value-creating activities through:

i. identifying potential threats that may cause adverse impacts on an organization's business operations and associated risks
ii. providing a framework for building resilience for business operations;

iii. providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and failures (ISO 247620: 2008).

1.7 Consequently, BCM is the entire organization's responsibility, which the enterprise risk management function must lead.

1.8 When planning for business continuity, the alternative arrangements for information processing and communication facilities (ICT service continuity) are essential for ensuring information, communication technology, and service availability during a disaster and serve as part of the base for the disaster recovery of activities going forward. Such fall back arrangements may include third parties in reciprocal agreements or commercial subscription services.

1.9 Despite the critical role played particularly by the information and communication technology (ICT) during the pandemic, the ability of this capability to maintain and salvage organizational operations during and after disruptions is proportional to the amount of planning that has been embarked upon preparation for such eventuality.

1.10 Furthermore, ICT service continuity planning is squarely dependent on a functional BCMS of the organization. Departments must understand that any ICT service continuity arrangements in the absence of a fully functional BCMS might not yield the desired outcomes.

1.11 Consequently, this determination and directive, therefore, assume that departments already have Business Continuity Plans (BCP) as per the provisions of the Corporate Governance of Information and Communication Technology Policy Framework (CGICTPF). The BCP must, amongst other things, identify and or cover minimum critical services that shall continue to be provided by a department even during a disaster. In line with this, the determination and directive focus on information and communication technology fallback arrangements for departments during a disaster.

2. PURPOSE

2.1. The purpose of this Determination and Directive is to provide clear guidance to departments for the development and implementation of ICT service continuity plans in support of the Department's Business Continuity objectives.

2.2. The above is done to ensure the continued availability of ICT systems and services during the disruption and the ability to recover quickly upon being impacted by the disaster.

3. AUTHORIZATION

The Minister for Public Service and Administration (MPSA) issues this Determination and Directive in terms of section 3(2), read with sections 3(1)(f), and (g) of the Public Service Act, 1994.

4. SCOPE OF APPLICATION

This Determination and Directive applies to all national and provincial departments, government components, and employees employed in terms of the Public Service Act. This Determination and Directive shall only apply to members of the services, educators or members of the Intelligence Services only in as far as the provisions of this Determination and Directive are not contrary to the laws governing their employment.

5. IMPLEMENTATION OF THE DETERMINATION AND DIRECTIVE

5.1 The Head of Department must ensure that the current ICT Service Continuity Plan aligns with the contents of this Determination and Directive.

6. NON-COMPLIANCE MANAGEMENT

Failure to comply with this Determination and Directive will be dealt with in line with the provisions of section 16A of the Public Service Act.

7. DATE OF IMPLEMENTATION

This Determination and Directive shall come into effect on the date of signature by the MPSA.

8.1 CURRENT MINIMUM ICT REQUIREMENTS

8.1.1 The Head of Department must establish an ICT Disaster Recovery Team for the department. The ICT Disaster Recovery Team led by the GITO will develop, document, and execute processes for a department's data recovery f of business continuity, and IT infrastructure in the event of a disaster/ ICT service / ICT system disruption.

8.1.2 Guided by the risk appetite and tolerance of the department, the ICT Disaster Recovery Team must define and agree on what would constitute as an ICT disaster.

8.1.3 The Head of Department, through the office of the GITO must identify all departmental Information Systems / ICT Services supporting both internal operations and service delivery to the public, customers, and stakeholders.

8.1.4 The Head of Department must determine the impact of Business Impact Analysis (BIA) on the department and the public/customers/stakeholders should each of the identified

information systems / ICT Services, referred to in paragraph 8.1.3, not be provided due to disruption/disaster.

8.1.5 The Head of Department must determine the system availability/capacity requirements of the department informed by the BIA or their criticality.

8.1.6 The Head of Department must ensure that redundancy/continuity arrangements are in place and informed by the department's system availability/capacity requirements.

8.1.7 The Head of Department must ensure that the unavailability of critical information systems, as identified by the BIA process, is captured in the department's strategic and operational risk registers.

8.1.8 The Head of Department must inform all relevant stakeholders when an ICT disaster is declared, including the GITO.

8.1.9 The Head of Department must identify the minimum critical ICT services that must be provided by the department even during the disruption/disaster.

8.1.10 The Head of Department must determine the duration within which critical ICT services Recovery Time Objectives (RTO) must be recovered should a disaster/disruption occur, this must be expressed in minutes, hours, or days.

8.1.11 The Head of Department must determine the recovery point and the associated data/information that must be retrieved during the disaster. The Recovery Point Objectives (RPO) after the disaster/disruption must be expressed in minutes, hour and days in case of future disruptions.

8.1.12 The Head of Department must ensure the existence and safekeeping of all relevant documentation that will support disaster recovery efforts by the department. Such documents must include but are not limited to the design and configuration of the system documents primarily for critical and other systems, systems recovery procedures, contact details of staff (including 3rd party contractors) to assist/conduct recovery, relevant 3rd party suppliers, etc.

8.1.13 The Head of Department must provide an alternative ICT workspace/working environment for employees/recovery teams.

8.1.14 The Head of Department must ensure that communication mechanisms of the department determine roles and responsibilities to be performed by various stakeholders once the disaster/disruption strikes.

8.1.15 At a minimum, during the development of the ICT Service Continuity plan, the following must be addressed:

a) **The overview of the department's ICT Infrastructure**

The GITO must establish an inventory of the status quo of the environmental ICT infrastructure. This inventory list must include:

i Hardware
ii Software (Including Applications)
iii Network information assets (i.e., Servers, Switches, Firewalls, Routers, Virtual Machines)
iv Network Diagram/Blueprint of the department

b) **Backup Procedures**

The GITO must establish a process of creating and storing copies of data that can be used to protect the department against data loss.

c) **Service and System Risk Ratings**

The GITO must ensure that all the information systems are rated in their criticality/importance (High, Medium, Low) informed by the BIA outcome.

d) **The ICT Disaster Recovery Process**

The GITO must identify and prioritize their business functions, maintaining the ICT systems that support their operations. The recovery arrangements must also be established to preserve the continuity of ICT services.

e) **Roles and Responsibilities**

The GITO must ensure that the roles and responsibilities related to the ICT services continuity plan are clearly defined and known to those responsible for implementing the disaster recovery activities.

f) **Key Contacts**

The GITO must ensure that critical contacts are continuously updated and accessible when needed.

g) **Testing and Maintenance of the ICT Service Continuity Plan**

The GITO must ensure that the ICT Service Continuity Plan is tested and maintained regularly for effectiveness.

h) **Review Date of the ICT Service Continuity Plan**

The GITO must ensure that the ICT Service Continuity Plan is reviewed regularly and when required.

8.2 DURING THE ICT DISASTER

8.2.1 The ICT Disaster Recovery Team must invoke the disaster recovery activities, processes, and procedures as stipulated in the ICT Service Continuity Plan.

8.2.2 The ICT Disaster Recovery Team must ensure that the respective role players are informed (including third parties and suppliers).

8.2.3 The ICT Disaster Recovery Team must ensure that continuous touch point conversations are convened to ensure ongoing engagements during the disaster.

8.3 AFTER THE ICT DISASTER

8.3.1 At the end of the disaster, the Head of the Department must ensure that the ICT disaster recovery team conducts a post-implementation review.

8.3.2 The Head of Department must ensure that the disaster has been declared over and normal operations are resumed.

APPROVED BY THE MINISTER FOR THE PUBLIC SERVICE AND ADMINISTRATION

_____
MR T.W. NXESI, MP
ACTING MINISTER FOR THE PUBLIC SERVICE AND ADMINISTRATION
DATE:

The GITO must ensure that the ICT Service Continuity Plan is tested and maintained regularly for effectiveness.

h) **Review Date of the ICT Service Continuity Plan**

The GITO must ensure that the ICT Service Continuity Plan is reviewed regularly and when required.

8.2 DURING THE ICT DISASTER

8.2.1 The ICT Disaster Recovery Team must invoke the disaster recovery activities, processes, and procedures as stipulated in the ICT Service Continuity Plan.

8.2.2 The ICT Disaster Recovery Team must ensure that the respective role players are informed (including third parties and suppliers).

8.2.3 The ICT Disaster Recovery Team must ensure that continuous touch point conversations are convened to ensure ongoing engagements during the disaster.

8.3 AFTER THE ICT DISASTER

8.3.1 At the end of the disaster, the Head of the Department must ensure that the ICT disaster recovery team conducts a post-implementation review.

8.3.2 The Head of Department must ensure that the disaster has been declared over and normal operations are resumed.

APPROVED BY THE MINISTER FOR THE PUBLIC SERVICE AND ADMINISTRATION

MR T.W. NXESI, MP
ACTING MINISTER FOR THE PUBLIC SERVICE AND ADMINISTRATION
DATE: 29/11/2022