MBEYA UNIVERSITY OF SCIENCE AND TECHNOLOGY

GUIDELINES FOR ICT SECURITY INCIDENCE MANAGEMENT

AUGUST 2023

FOREWORD

Mbeya University of Science and Technology (MUST) is a Public Institution established through the Universities Act NO. 7 of 2005 and the MUST Charter GN 452A of 2013 aiming at becoming the leading Centre of excellence for knowledge, skills and applied education in science and technology through training, research and consultancy. Currently, MUST has developed ICT Incidence Management Guidelines of 2023 that guides against threat to the security of the University's ICT systems.

The Guidelines is also developed to implement other Government and sectoral policies including the National Information and Communications Technology Policy 2006 and Government Cyber Security Strategy 2022–2027.

The success in achieving the objectives of the Guidelines is the responsibility of all actors at the University. However, Directorate of ICT has a vital role in its implementation.

The development of the Guidelines could not have been a success without the contribution of different stakeholders within MUST community, Staff and students. The University appreciates their great role in providing information, advice, and opinions to help in creating the Guidelines.

It is hoped that the Guidelines for ICT Security Incidence Management will go a long way in addressing and providing guidance in all ICT security incidences at the University.

Prof. Aloys N. Mvuma

Vice-Chancellor
Mbeya University of Science and Technology

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

CIO	Chief Information Officer
DVC-ARC	Deputy Vice Chancellor-Academic Research and Consultancy
DVC-PFA	Deputy Vice Chancellor-Planning Finance and Administration
DICT	Director of Information and Communications Technology
ICT	Information and Communications Technology
M&E	Monitoring and Evaluation
MUST	Mbeya University of Science and Technology
VC	Vice Chancellor

DEFINITION OF KEY TERMS AND CONCEPTS

Academic Staff: Academic Staff are professors, lecturers, tutorial assistants, instructors and research fellows who are employed by the University, whether on full time or part time, permanent or temporary.

Administrative Staff: Administrative Staff are persons who are employed by the University and are determined by the University Council to be members of Administrative Staff.

ICT Security Incidence: Any event that poses a threat to the security of an organization's information or IT systems.

INTRODUCTION

1.1. Background

Mbeya University of Science and Technology (MUST) is a result of the transformation of the Mbeya Institute of Science and Technology (MIST) in accordance with the Universities Act NO.7 2005 and Mbeya University of Science and Technology Charter GN 452A of 2013.

Vision

The Vision of Mbeya University of Science and Technology is to become the leading centre of excellence for knowledge, skills and applied education in science and technology.

1.2. Mission

The Mission of Mbeya University of Science and Technology is to develop academically, technologically and socially competent students, staff and other stakeholders who will be responsive to the broader needs and challenges of the society specified through the following objectives;

(a) Facilitating appropriate tuition, practical training and support according to the needs of students and other customers;
(b) Encouraging staff commitment to quality education and services including research, consultancy and innovation;
(c) Fostering lifelong learning, honesty and responsibility;
(d) Promoting environment conducive for human development; and
(e) Promoting effective entrepreneurship and usage of appropriate technology that meet national and international needs and standards through skills and practical oriented training, research and consultancy.

1.3. Strategic Mandate

Strategic mandate of the University is derived from the phrase “Science and Technology” in its name. This mandate is to provide tertiary and higher

education, promote technology development, undertake research and consultancy, disseminate knowledge and foster relationships with other agencies for development of the nation.

1.4. MUST Motto

Endeavouring to lead in Science and Technology.

1.5. Directorate of Information and Communications Technology

The Directorate of ICT started in 2020 being a result upgrading of System Administration Unit and later Centre for Networking and Computing. The Directorate has the function of coordinating, directing and managing Information and Communications Technology (ICT) and related issues at the University.

1.6. Justification of ICT Security Incidence Management

The adoption of ICT to MUST business process is important in order to improve service delivery and attain competitive advantage. ICT in education improves engagement and knowledge retention: When ICT is integrated into lessons, students become more engaged in their work. This is because technology provides different opportunities to make it more fun and enjoyable in terms of teaching the same things in different ways.

However, the automation of MUST business process brings new ICT security challenges. The threats that are brought from the adoption and development of ICT services need to be managed. The threats are identified as ICT security incidences. When proper incidence management measures are in place damage can be managed and risk can be reduced to the organization. Incident management also helps organizations quickly identify attacks.

1.8. Benchmarking

This Guidelines have adopted the International Standard of Information Technology Infrastructure Library (ITIL). ITIL is the framework of best practices for delivering Information Technology (IT) services.

2.0. ICT SECURITY INCIDENCE ROLES AND RESPONSIBILITIES

The ICT security incidence management consists of the following participants:

(a) Security Incident Manager;
(b) Security Analyst;
(c) Information security team and
(d) Incident handler.

2.1. Roles and Responsibilities

The following are roles and responsibilities of incident management team;

(a) **Security Incident Manager/Director of ICT:** The person is responsible for coordinating the response to the incident. They will work with all other team members to ensure that the incident is dealt with efficiently and effectively.

(b) **Security Analyst/ICT Officer:** The security analyst is responsible for investigating the incident and gathering all relevant information. They will work closely with the security incident management to understand the scope of the incident and determine the best course of action.

(c) **Incident handler/ICT Officer:** The person in charge of organizing resources and handling communication when responding to a security incident. The first responder should perform the function to the best of their knowledge, skills, and abilities up until an Incident Handler has been identified.

(d) **Information security team/ICT Officers Team:** The team comprises of security incident management.

3.0. SECURITY INCIDENCE MANAGEMENT

The process flow will involve the step-by-step flow diagram from when an event is noted to the closing of an incident, the parties involved, their duties and best practices.

3.1. Process Flow

The ICT security incidence management will follow the following flow shown in Figure 1.

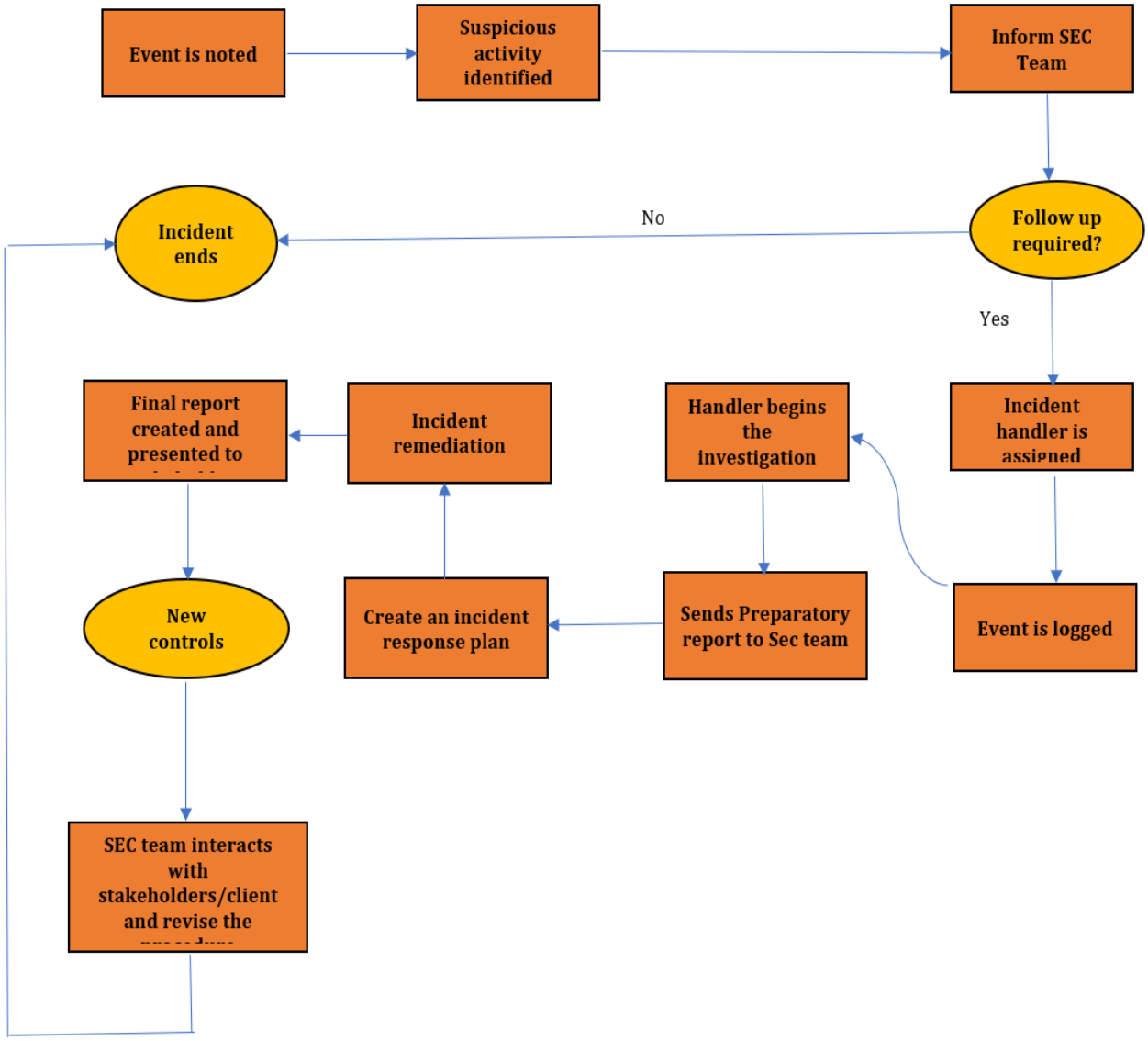

Figure1: Flow of ICT security incidence management

3.2. Best Practices

The following parameters will be monitored and evaluated:

(a) The Information Security Officer, in collaboration with the ICT Officers, will create an "Information Security Incident Management Form" to report all security violations/occurrences and to create a swift reaction mechanism for information security incidents.

(b) All workers must understand and be able to recognize any strange or unexpected behaviour on the assets that could indicate a software failure. The following are examples of security occurrences, though they are not exhaustive:

(i) System alterations that are uncontrollable.

(ii) Inadequate access (e.g., password sharing).

Physical security breaches are:

(a) Hacking or manipulation of systems;

(b) Confidentiality of data is jeopardized (e.g., data theft);

(c) Data integrity is jeopardized (i.e., damage to data or unauthorized modification);

(d) Misuse of data, assets, or services;

(e) Infection of a system with a malicious or illegal program;

(f) An effort to gain access to a computer without authorization;

(g) Changes to hardware, software, or infrastructure configuration that are not approved/authorised;

(h) If a security incident is discovered, users must take the following steps;

(i) Take note of the symptoms and any error messages that appear on the screen.

(j) If an infection is suspected, disconnect the workstation from the network (with the help of the ICT Officer);

(k) Do not utilize any contaminated removable media (e.g., USB memory sticks).

All staff and students are required to notify the DICT of any suspected security-related events. Information such as, but not limited to the following must be provided:

(a) The individual who reported the incident's name and phone number;

(b) The type of data or equipment that is being used;

(c) Whether the loss of the information poses a threat to any individuals or other data;

(d) The incident's location;

(e) Any impacted equipment's inventory numbers;

(f) The time and date of the security breach;

(g) The location of the affected data or equipment; and

(h) The incident's type and circumstances.

4.0. RESPONSIBILITIES IN MONITORING AND EVALUATION

4.1. Top Management Team

The top Management team consists of Vice Chancellor, Deputy Vice Chancellor Academic, Research and Consultancy (DVC-ARC) as well as Deputy Vice Chancellor Planning, Finance and Administration (DVC-PFA). They have a big role to play in monitoring and evaluation of incidence management through close follow up and decision making on reported incidences which requires top management interventions.

4.1.1. Vice Chancellor

(a) As the Chief Executive Officer of the University, among other roles, the Vice Chancellor is responsible on day-to-day ICT implementation;

(b) Ensure short, medium- and long-term implementation of ICT; and

(c) Approve financial and other resources for the implementation of the guidelines.

4.1.2. Deputy Vice Chancellor-Academic Research and Consultancy

Assist in the coordination between colleges, academic centers, units and departments with the directorate of ICT in implementation of the guidelines.

4.1.3. Deputy Vice Chancellor-Planning, Finance and Administration

(a) Ensures that qualified ICT Officers are employed, developed and capacity building based on ICT security current requirements;

(b) Lead coordination of the ICT security and guidelines implementation;

(c) Recommend approval of appropriate new ICT security incidences control measure; and

(d) Ensure the operationalization of the work plan.

4.1.4. Director of ICT

(a) Ensure day to day implementation of the Guidelines;

(b) Audit, report and advice Top Management on ICT security incidences related to the University operations;

(c) Compile various incidences reported from stakeholder, stakeholders' reports and propose way forward and

(d) Check on capacity building, coordinate, prepare, facilitate seminars and training related to ICT security.

4.1.5. Principals and Directors

The role of Principals and Directors in making College and Directorate benefit from ICT are:

(a) Act as a central role in College and Directorate in reporting any ICT security incident to the DICT;

(b) Encourage College members of staff to be ethical on ICT resource utilization.

4.2. Review of Guidelines

The Guidelines will be reviewed after four (4) years. Prior to that, they may also be reviewed from time to time as deemed necessary.

5.0. PARAMETERS TO BE MONITORED

In order to monitor ICT Security Incidence Management Guidelines, the following parameters will be observed;

(a) ICT Security Incidences noted;
(b) Following of Process Flow and
(c) Participation of Key Players in handling Incidences.

5.1. Indicators for Monitoring

The following will be regarded as evidence for monitoring and evaluation of Incidents Management:

(a) Recorded and categorized incidences in accordance to priority and urgency;
(b) Number of Reports written after closing the incidence;
(c) Report on student/staff ratio and teaching load each semester and
(d) Lesson learned during resolving the incidences.

5.2. Monitoring Tools

ICT Incidents will be monitored and evaluated through the use of a checklist.

REFERENCES

Government Cyber Security Strategy 2022–2027 (EIGE).

Mbeya University of Science and Technology Information and Communication Technology Policy (2020).

National Information and Communications Technology Policy (May 2016)

APPENDICES

APPENDIX 1

IT Security Incident Report			
Report details			
Report Date:			
Report Number:			
Created by:			
Role:			
Incident Details			
Date of incident:			
Time of Incident:			
Incident Type:			
Location of Incident:			
Status of Report:			
Incident Description:			
People affected by the Incident			
Name	**Role**	**Equipment Affected**	
Follow up actions			
Action	**Responsible**	**Comments**	

Approval of Documentation	
Name	
Role	
Date of Approval	
Signature:	

APPENDIX 2

	MBEYA UNIVERSITY OF SCIENCE AND TECHNOLOGY	

Incident Report

Organization:			
Department:			
Section:		**Sheet:**	

Initial Incident Details			
Incident Raised By:		**Incident Received By:**	
Report Date:		**IT Service Disrupted:**	

Detailed Incident Information			
Incident Date:		**Incident Hour:**	
Incident Number:		**Incident Category:**	
Was the SLA Breached?		**Duration of Interruption:**	

Incident Description

Business Impact

Corrective Actions Taken

Lesson/s Learned

Authorization			
Authorized By:		**Position:**	
Date:		**Signature:**	