UNIVERSITY OF DAR ES SALAAM

Information and Communication Technologies Security Policy (2022)

May 2022

Plan Approval

University of Dar es Salaam ICT Security Policy

Reference	*UDSM_ICTSP_2022*
Version	1.0
Prepared by	UDSM Directorate of ICT
Owned by	University of Dar es Salaam
Approved by	University Council
Date Approved	14th June, 2022
Name and Title	
Signature	
Remarks	

Table of Contents

List of Abbreviations and Acronyms

ISP	ICT Security Plan
BC & DRP	Business Continuity and Disaster Recovery Plan
CIA	Confidentiality, Integrity and Availability
CSERT	Computer Security Emergency Response Team
ComPAR	Computer Publicly Accessible Rooms
CSIRT	Computer Security Incident Emergency Response Team
DICT	Directorate of Information and Communication Technologies
eGA	e-Government Authority
ICT	Information and Communication Technology
UDICTSP	UDSM ICT Security Policy
ISC	Information Security Classification
ISP	ICT Security Plan
OLA	Operational Level Agreements
SLA	Service Level Agreement
SPIRT	Security Policy Implementation and Review Team
SOP	Standard Operating Procedures
SRAMT	Security Risk Assessment and Mitigation Team
UAT	User Acceptance Testing
UDSM	University of Dar es Salaam
UDSMNet	UDSM Local Area Network

Glossary

Accountability	Associating a specific action with an individual.
Approved software	Software that has been reviewed and deemed acceptable by an authority for use with its ICT resources
Anti-malware software	Software installed on a computing device to protect it from malicious software.
Application	a software program or group of software programs designed to work together to accomplish specific business objectives
Asset Custodian	An individual that has responsibility for the security of data and applications in an information asset.
Audit logs	Documentation of user activity on an ICT resource. Logs could have information such as date, time, action, and account details
Authorization	the process of determining whether or not an identified individual or group has access rights to an information resource, and determining what type of access is allowed, e.g., read-only, create, delete, and/or modify.
Authentication	the process of confirming that a known individual/ system is correctly associated with a given electronic credential, for example, by use of passwords to confirm correct association with a user or account name.
Business System	any information system that is critical to the on-going operations of the University and would cause losses to the University if data integrity is compromised or if the system becomes unavailable.
Critical Information Resources	Resources determined by the University management to be essential to its critical mission and functions, the loss of which could have an unacceptable impact
Data store	A collection of information organized in such a way that it can be accessed, managed, and updated.
Hardware Failure	refers to the failure of ICT equipment such as a computer or its storage devices.
ICT	Any communication device or application, including radio, television, cellular phones, computer and network hardware and software, as well as satellite systems and associated services and applications.
ICT Security Policy	A document that provides high-level statements about organizational beliefs, goals, objectives, and resolutions about ICT security.
Securit*y*	Ensuring confidentiality, integrity, and availability of information assets:

	● **Confidentiality**- Ensuring that information is accessible only to those authorized to have access; ● **Integrity-** Safeguarding the accuracy and completeness of information and processing methods for information; ● **Availability:** Ensuring that authorised users have access to information and associated assets when required.
Security Incident	Any action or activity that compromises the confidentiality, integrity, or availability of ICT resources.
Service providers/ contractors	Persons/organisations that provide ICT services to ***Users* of ICT** include but are not limited to: ● All Students and University Staff; ● Other persons and organisations working with or on behalf of the University; ● Any other person who has been explicitly registered as a user of any of the University's ICT assets or computer networks, or who has otherwise been explicitly authorized to use such assets; ● Any other person accessing or attempting to access any University ICT asset to which public access has been provided; and ● Any other person using the University's ICT assets to do business with the University, whether as a researcher, contractor, consultant or supplier.
Information Asset	Refers to any data or information, as well as related equipment that contains or processes data or information that is relevant to the University functions.
Information Security Classification	Categorisation of an information asset for the purpose of identifying the security controls required to protect that asset
Information Security	Refers to the preservation of Confidentiality, Integrity, and Availability to ensure that information and associated services are available to authorized users when required
IT Infrastructure	Network devices, server hardware, and host operating systems
IT Resources	Refers to computer hardware, software, networks, computing devices, information systems, applications, and data.
Least Privilege	The principle that grants minimum possible privileges to permit a legitimate action, in order to enhance protection of data and functionality from malicious behaviour.
Malware	Malicious software
Mobile	A laptop, PDA, or other portable device that can process

Computing Device	data.
Peer to Peer	Communication model that allows direct sharing of files (audio, video, data, and software) among computers.
Remote Access	Any access to the UDSM network through a network, device, or medium that is not controlled by the agency (such as the Internet, public phone line, wireless carriers, or other external connectivity).
Risk Analysis	A process that systematically identifies valuable information system resources and threats to those resources, quantifies loss exposure (i.e., loss potential) based on the estimated frequency and cost of threat occurrences, and recommends how to allocate resources for applying countermeasures to minimize total exposure. The analysis lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first.
Risk Assessment	The process of doing cost-benefit analysis to information technology resources, associated security risks, and mitigation strategies.
Security Controls	Hardware, software, programs, procedures, policies or physical safeguards implemented to fulfil security requirements and mitigate risks to information technology resources**.**
Separation of Duties	The concept of requiring more than one person to complete a task. It is a way to ensure that no one individual has the ability to control an entire process.
Segregation of duties	A method for reducing the risk of accidental or deliberate system misuse. Separating the management or execution of certain duties or areas of responsibility in order to reduce opportunities for unauthorized modification or misuse of information or services.
Service Account	An account used by a computer process (e.g., an account used by the back-up process for file access).
Standards	A specific set of practices or procedures to regulate how a system or organization provides services. This may include a list of configurations, software or hardware.
Visitor	Any person who accesses an ICT system, service or equipment that is owned, managed or supplied by UDSM or one of its partners, but is not a UDSM student or member of staff.

1. Introduction

The University of Dar es Salaam (UDSM) has been investing in Information and Communication Technologies (ICT) resources in an effort to improve its teaching, learning, research, service delivery, and administrative functions. The University has procured and implemented ICT facilities that are used to create, process, store, and share data and information. This infrastructure is used to support running of different software systems, which hold vital information. All these are assets that represent a significant investment by UDSM. Their continued availability in support of UDSM core business functions is of utmost importance. Hence, there is a need to secure and control their access to ensure confidentiality, integrity and availability.

Investing in ICT resources comes with its own challenges because the University ICT environment could be exposed to cyber security threats. An attack on UDSM ICT resources could cause reputational harm to UDSM and could affect core operations of the University. Thus, a special consideration should be given to ICT security, if the University community is to benefit from investing in ICT. The University has, therefore, decided to introduce this policy to manage the risks associated with ICT.

This document defines the security policy for ICT resources across UDSM campuses. The ICT resources implied in this document include ICT network infrastructure, system software, information systems, computing devices, CCTV camera systems, printing facilities, and data/ information transmitted and stored in electronic format. These resources are extremely valuable for the day-to-day discharge of core business and administrative functions of the University. The ICT security policy will enable the University to securely carry out its activities, by protecting and preserving University ICT assets at appropriate levels of security. The policy is built on the core principles of information security, namely Confidentiality, Integrity, and Availability.

The University has just revised its ICT Policy of 2006 to set new ICT strategic directions in response to the current and future ICT needs of the University Community, changes in the ICT field, and national development agenda. The following are the current ICT vision and mission of UDSM as stipulated in the UDSM ICT Policy (2022).

- **UDSM ICT Vision:** Harnessing the full potential of ICT as an enabler to transform UDSM into an e-University, and support the national development agenda in building a digital economy.

- **UDSM ICT Mission:** Upgrading and developing UDSM ICT resources and strengthening their use in discharging core business and administrative functions, and enhancing ICT research, innovation, training and industry collaboration to actively contribute to the national ICT strategic priorities.

Therefore, following the introduction of the revised UDSM ICT Policy (2022-2031), it was necessary for the University to review its ICT Security framework. This ICT Security Policy (UDICTSP) is expected to guide the necessary measures to be taken to secure UDSM ICT resources for the period of 2022 to 2026. The implementation of this policy will necessitate the development and enforcement of various rules, guidelines, standards, and procedures to guide access and use of the University's critical business information assets and associated ICT resources.

2. Purpose

The UDSM is implementing this ICT Security Policy to protect the Confidentiality, Integrity, and Availability (CIA) of institutional data, information systems that store, process and/or transmit institutional data, and other ICT resources.

3. Scope and Target Audience

This policy applies to all users of UDSM ICT critical information assets and ICT resources, which include the following:

i. ICT network infrastructure and the related network services;
ii. ICT facilities such as desktop computers, computer labs, computer publicly accessible rooms (ComPAR), electronic whiteboards, laptops, printers, photocopiers, scanners, removable storage media, and mobile computing and tele-working devices;
iii. Security control systems such as CCTV camera systems;
iv. Information systems used for research, teaching, learning, delivery of public services, and administrative functions;
v. System software such as operating systems and software development kits;
vi. Specific application software such as antimalware, data analysis packages, reference managers, and office applications;
vii. Data generated, transmitted and/or stored in the UDSMNet.
viii. ICT services such as the Internet, email system, and telephony system; and
ix. Any other system that may be installed to provide a service on the UDSMNet.

This policy recognises the following three categories of users of UDSM ICT resources.

i. Main users: students enrolled across all UDMS campuses, and permanent UDSM staff.
ii. Temporary users: temporary, casual or agency staff working for or on behalf of the University.
iii. Third party users: contractors, consultants and suppliers working for or on behalf of the University, partner institutions, and visitors of the University who could be given access to UDSM ICT resources.

4. ICT Security Principles and Policy Statements

To effectively achieve the CIA of UDSM critical information assets and ICT resources, the ICT security control principles and best practices were adapted from ISO 27000 series of standards and the technical guide on developing ICT security policies from the Tanzanian e-Government Authority (eGA). The principles were adapted to the UDSM ICT environment. Thus, based on these principles and best practices, critical issues related to the security of UDSM ICT environment were identified and the respective objectives were formulated. Thereafter, policy statements to address critical ICT security issues were formulated. The subsequent sections provide descriptions of the ICT security principles and the corresponding policy statements.

4.1. Principle I: ICT Security Policy, Planning, Governance and Management

4.1.1. Aim

The aim of this security control principle is to establish effective ICT security planning and governance, in line with the University business goals and objectives, in order to ensure efficient, effective and equitable use of current and future ICT resources.

4.1.2. Policy Statements

The University shall:

a. Develop an ICT Security Plan (ISP) that aligns with the University business plan, general security plan and risk assessment findings.
b. Establish processes for the review, assessment and prioritisation of existing and future ICT security strategies and plans, as well as the communication of these strategies and plans.
c. Establish and document internal information security governance and management mechanisms, including roles and responsibilities to implement, maintain and control the operations of information security within the University.
d. Establish and document external information security governance mechanisms to ensure that third party service level agreements (SLAs) and operational level agreements (OLAs) clearly articulate the level of security required and are constantly monitored.
e. Define a set of policies for ICT security, which shall be approved by the UDSM management, and published and communicated to members of the UDSM community and relevant external parties.
f. Review the ICT security policies at the planned intervals, as defined in Section 4.11.2(h of this document, or at any time if significant changes occur, to ensure their suitability, adequacy and effectiveness.
g. Maintain appropriate contacts with relevant law enforcement authorities.

h. Ensure that ICT security is addressed in ICT related projects, including software development and support processes, to maintain the security of software and systems, applications, business information, projects, and support environments.
i. Integrate ICT security risk management--risk assessment, treatment, acceptance, communication and monitoring and evaluation--into the Enterprise Risk Management Framework.

4.2. Principle II: ICT Security Operations & Communication Management

4.2.1. Aim

The purpose of this principle is to ensure correct and secure ICT operations, and managing the communication of information processing facilities.

4.2.2. Policy Statements

The University shall:

a. Establish standard operating procedures (SOPs) for managing and operating all information processing facilities. This shall include the development of appropriate operating instructions and incident response procedures.
b. Develop and implement operational procedures for change management. The procedures shall consider identification and recording of significant changes, assessment of the potential impact of such changes, formal approval procedure for proposed changes, communication of change details to all relevant parties, and identifying responsibilities for aborting and recovering from unsuccessful changes.
c. Monitor the use of ICT resources, make optimization and projections of future requirements to ensure best performance.
d. Implement procedure for segregation of duties where appropriate, to reduce the risk of negligent or deliberate system misuse. The procedures shall be treated as formal policy documents and the responsible authority must authorize changes. They will specify the instructions for processing and handling of information, scheduling requirements, instructions for handling errors, support contacts in the event of unexpected operational or technical difficulties, special output handling instructions, and system restart and recovery procedures for use in the event of system failure.
e. Implement detection, prevention and recovery controls to protect UDSM ICT resources against malware. Additionally, the University shall conduct security awareness programs, to ensure that all users are aware of the security threats and their mitigation measures.
f. Develop and implement procedures for housekeeping activities associated with information processing and communication facilities. Such activities include procedures for starting and shutting down of computers, data backup, maintenance of devices, and management and safety of computer room and e-mail services.

g. Develop procedures for producing, keeping and regularly reviewing event logs for user activities, exceptions, faults and ICT security events. Logging facilities and logged information shall be protected against tampering and unauthorized access. The procedures shall consider identifying and recording significant changes, assessing potential impact of such changes, formal approval procedure for proposed changes, communicating change details to all relevant parties, and identifying responsibilities for aborting and recovering from unsuccessful changes.
h. Synchronize to a single reference time source all clocks of all relevant information processing systems.
i. Ensure availability of information about technical vulnerabilities of information systems being used, and take appropriate measures to address associated risks.
j. Establish and implement standard operating procedures to govern the installation of software by end users.
k. Carefully minimise disruptions to UDSM business by developing ICT audit requirements and activities for verification of operational systems. Any events shall be reported immediately to the ICT service desk either by email, telephone or any other appropriate means.
l. Identify security mechanisms, service level agreements and management requirements of all network services, irrespective of whether these services are provided in-house or outsourced.
m. Appropriately protect UDSM information involved in electronic communication.
n. Develop and implement procedures to govern separation of duties between development and operational facilities as lack of separation may pose potential security threats, including a possibility of compromising, damage, or loss of data at the contractor's site. Risks shall be identified in advance, and appropriate control measures shall be articulated within a particular SLA.

4.3. Principle III: ICT Assets Management Security

4.3.1. Aim

The principle aims at ensuring that all University information is assessed to determine its sensitivity and to ensure that all information assets are provided with appropriate control and protection.

University Information assets shall be classified into one of the following:

a. **Public** – information that can be accessed by the general public (e.g., contents of websites);
b. **Internal** – information about university activities; the application and use of this information is relevant to the University community only.
c. **Restricted** – information generated or utilised when performing University functions that are associated with specific restrictions, institutional risks, and legal requirements.

4.3.2. Policy Statements

The University shall:

a. Ensure that each information asset is given an Information Security Classification (ISC) identifier, so that it can be managed and secured in a manner that is appropriate for its sensitivity and/or importance.
b. Classify information assets in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
c. Ensure that each of its information systems is uniquely identified and assigned to a particular an Asset Custodian as per the ISC policy and procedures.
d. Ensure that all its information assets are inventoried, and custodians are accountable for the security of their information assets.
e. Develop and implement a policy for acceptable use of information assets, and identify and document assets associated with information and information processing facilities.
f. Ensure that all employees and third-party users return ICT assets in their possession immediately after they stop working for UDSM, and their access rights to UDSM ICT facilities are revoked.
g. Ensure that procedures for management of removable media are implemented in accordance with the classification scheme adopted for removable media.
h. Ensure that all media containing critical information are protected against unauthorised access, misuse or corruption during transportation in and out of the University.
i. Ensure that all information on storage media is securely managed, controlled, moved and disposed, in such a way that the information content is not disclosed;
j. Enforce the use of cryptographic controls to ensure confidentiality, authenticity and/or integrity of critical information assets and ICT services that are considered to be at risk and for which other controls do not provide adequate protection.

4.4. Principle IV: Identity and Access Control Management

4.4.1. Aim

The principle aims at ensuring adequately control access to UDSM critical business information assets and ICT resources.

4.4.2. Policy Statements

The University shall:

a. Develop and maintain a policy to govern access control for its business processes and functions. The policy shall take care of access control rules and rights for each user or group of users, security requirements of individual business applications, identification of all information related to specific business applications, policies for information dissemination and authorisation, consistency between access control and information classification policies of different systems and networks, and relevant legislation and any contractual obligations regarding protection of data or services against unauthorised access.

b. Enforce user access control and management of privileges. In addition, UDSM shall put formal procedures in place to control the allocation of access rights to information systems and services. The procedures shall cover all stages in the life cycle of user access, from registration of new users to de-registration of users who are no longer entitled to access business information assets and other ICT resources.
c. Enforce a code of responsibility for users with access to UDSM ICT services, to prevent unauthorised user access. Users shall be made aware of their responsibilities, to ensure effective access and use of UDSM ICT services, particularly regarding the use of passwords and the security of user devices.
d. Enforce protection mechanisms for unattended user devices. Users shall ensure that any unattended equipment has appropriate protection. Equipment such as workstations and file servers that are installed in user areas may require specific protection from unauthorised access when left unattended for an extended period. All users and contractors shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.
e. Enforce network access control policy to protect networked services from both internal and external threats. This is necessary to ensure that users who have access to the UDSM network do not compromise the security of these network services. This will be possible by ensuring that interfaces between the UDSM network and networks owned by other organisations or individuals have appropriate authentication mechanisms for users and equipment, appropriate mechanisms for remote user diagnostic, and control of user access to UDSM information services.
f. Enforce the usage of operating system access controls. Also, logical access to software systems and applications shall be restricted to authorized users. In addition, to prevent unauthorized computer access, security facilities provided by operating systems shall be used to restrict access to computer resources. The audit logs shall include information for identified and verified users, the terminal or location of each authorised user (if necessary), successful and failed system accesses, and connection times of users.
g. Enforce security for mobile computing and tele-working devices. To ensure information security when using mobile computing and tele-working facilities, the protection required shall be commensurate with the risks these facilities may cause. When using mobile computing devices, the risks of working in an unprotected environment shall be considered and appropriate protection measures shall be applied. In the case of tele-working, UDSM shall ensure that connections from tele-working sites do not compromise the security of UDSM network and ICT services.

h. Integrate ICT security risk management into the Enterprise Risk Management Framework. This includes risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and evaluation.
i. Periodically review users' access rights for all ICT resources.

4.5. Principle V: ICT Security Incidents and Response Management

4.5.1. Aim

This principle aims at preparing the University to adequately respond to, manage, and timely recover from ICT security incidents.

4.5.2. Policy Statements

The University shall:

a. Form a Computer Security Incident/emergency Response Team (CSIRT/CERT), which will be composed of staff members with appropriate expertise from the Directorate of ICT, legal unit, and selected academic units. The team shall be responsible for responding to ICT security incidents (real or suspected) by identifying and controlling them. Security incident findings shall be appropriately reported to the technical team in the DICT for proper measures and to the university management channels.
b. Define and apply procedures for the identification, collection, and preservation of information that can serve as evidence of security incidents.
c. Enforce mechanisms for ensuring that all events that could pose potential loss of data, breaches of confidentiality, unauthorised access or change of any system aspect are identified (event logging). Audit logs recording exceptions and other information about security events shall be produced and kept for an agreed period to assist in future investigations and monitoring of access control. Any event shall be reported immediately to the ICT service desk either by email, telephone or any other appropriate means.
d. Enforce SOPs/contingency plans for recovering, as quickly as possible, from all types of security incidents, including information system failures and loss of service, denial of service, and errors resulting from incomplete or inaccurate business data and breaches of confidentiality. The procedures shall also cover the analysis and identification of the cause of incident, planning and implementation of remedies to prevent recurrence, collection of audit logs and/or similar evidence (if necessary), communication with those affected by or involved in the recovery from the incident, and reporting the action to the appropriate authority.

4.6. Principle VI: ICT Security Business Continuity Management

4.6.1. Aim

This principle aims at ensuring that the University critical business information and ICT resources are free from any physical or logical security risk and/or disruption. It is critically important for the University deploy an ICT Business Continuity and Disaster Recovery Plan (ICTBC & DRP).

4.6.2. Policy Statements

The University shall:

a. Identify resourceful ICT personnel and periodically train them on how to execute the ICTBC & DRP.
b. Establish appropriate mechanisms to ensure that trained and authorised personnel perform ICTBC & DRP processes regularly and securely as defined in the corresponding SOPs.
c. Develop suitable ICTBC & DRP for critical business information assets and ICT resources. Subsequently, establish plans and processes for security risk and impact assessment of the loss of critical business information assets and ICT resources in the event of disaster. In addition, the University shall develop SOP for periodic review and update of critical business information assets and ICT resources.
d. Enforce control mechanisms to ensure that the ICTBC & DRP is periodically verified and reviewed to guarantee its effectiveness during adverse situations.
e. Ensure that information processing facilities are implemented with a redundancy level that is sufficient to meet availability requirements in case of disaster.

4.7. Principle VII: ICT Acquisition, Development, Deployment and Maintenance

4.7.1. Aim

This principle aims at ensuring that ICT security is a key consideration in the acquisition, development, deployment, and maintenance of ICT services at UDSM.

4.7.2. Policy Statements

The University shall:

a. Develop, implement, and monitor business security requirements in ICT services acquired or developed by UDSM. The security requirements shall include needs for fall back arrangements. Similar considerations shall be applied when evaluating software packages for business applications. It is worth noting that security controls introduced at the design stage are significantly cheaper to implement and maintain than those introduced during or after implementation.
b. Establish security requirements and appropriate controls that reflect the business value of all information assets, applications and involved ICT resources, and the potential business damage that might result from a failure or absence of security.

c. Establish a mechanism to prevent loss, modification, or misuse of user data in application systems. This shall include implementing appropriate controls and audit trails into application systems.
d. Enforce usage of cryptographic controls to protect confidentiality, authenticity and/or integrity of critical business information assets and ICT services that are considered to be at risk and for which other controls do not provide adequate protection.
e. The University shall enforce security of system files to ensure that ICT projects and support activities are conducted in a secure manner. Maintaining system integrity shall be the responsibility of the user or development group to whom the application or software belongs.
f. Enforce security in development and support processes so as to maintain security of systems and application software, business information, projects, and support environments. Persons responsible for specific application systems shall also be responsible for the security of the respective systems or support environment. They shall ensure that all proposed system changes are reviewed and tested to check that they do not compromise the security of either the system or the operating environment.
g. Enforce control mechanisms to monitor security vulnerabilities and threats for outsourced software development. When software development is outsourced, the following shall be considered: licensing arrangements; source code ownership and intellectual property rights; certification of the quality and accuracy of the work carried out; escrow arrangements in the event of failure of the third party; rights of access for auditing quality and accuracy of work done; contractual requirements for code quality; and user acceptance testing (UAT) before installation to detect trojan code, backdoors, and other security problems.

4.8. Principle VIII: Human Resource Security

4.8.1. Aim

The aim of this principle is to ensure that all human resources, including employees, students, suppliers, consultants and other parties involved understand their responsibilities and their roles in safeguarding the security of various UDSM information assets.

4.8.2. Policy Statements

The University shall:

a. Conduct background verification checks on all candidates for employment. The exercise shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed, and perceived risks.
b. Document and assign security roles and responsibilities in situations where employees and contractors have access to classified information or perform specific security related roles.

c. Ensure that security requirements are addressed during recruitment processes and in job descriptions.
d. Provide induction and on-going training on ICT security awareness to ensure that all users of UDSM information assets are well informed and understand the information security policy, their security responsibilities, and associated security processes.
e. Develop and implement procedures for scrutinising employee movement outside or within the University to ensure that, when appropriate, all ICT assets are returned and access rights are revoked. in accordance with the set regulations and terms of service.
f. Ensure formal and communicated disciplinary processes are in place to guide action against employees who commit ICT security breaches.
g. Ensure that ICT security responsibilities and duties that remain valid after one stops to work for UDSM are defined and communicated to all employees and contractors.

4.9. Principle IX: Physical and Environmental Management Security

4.9.1. Aim

The purpose of this principle is to prevent unauthorised access, damage and interference to the University business premises, business information assets, and ICT facilities. In addition, it aims to give precautions against disposition of ICT facilities as some are toxic when exposed to the environment such as sunlight and moisture.

4.9.2. Policy Statements

The University shall:

a. Ensure that all critical business information-processing facilities are housed in secure areas, and are protected by a defined security perimeter, with appropriate security barriers and entry controls. They shall be physically protected from unauthorised access, damage and/or interference.
b. Develop and implement SOPs to enforce physical access control and monitoring. The perimeter of a building, site containing critical information processing facilities, reception areas, offices, rooms or other sensitive areas should be clearly defined (i.e., there should be no gaps in the perimeter/areas where a break-in could easily occur). The external walls of the site shall be of solid construction and all external doors shall be suitably protected against unauthorized access.
c. Establish SOPs for equipment security control to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. They shall also include protection from power failures and disruptions caused by fire and flooding. Equipment shall be physically protected from security threats and environmental hazards. Protection of equipment (including equipment that are used off-site) is necessary to reduce the risk of unauthorized access to data and to protect them against loss or damage.

d. Design and apply physical protection of ICT resources against natural disasters, malicious attacks, or accidents.
e. Ensure access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
f. Establish SOPs for environmental safety management, secure disposal, or re-use of equipment. This shall include procedures for sanitization of ICT facilities or any sensitive data and licensed software prior to disposal or re-use. All processes should be done in ways that are friendly to the environment. Special controls may be required to protect ICT facilities against hazards or unauthorised access, and to safeguard supporting facilities such as electrical supply equipment and cabling infrastructure.
g. Implement clear guidelines for disposal of papers and removable storage media and a clear screening policy for information processing facilities.

4.10. Principle X: ICT Security Risk Assessment and Treatment Management

4.10.1. Aim

This principle aims at putting in place appropriate security measures that would ensure a university-wide secure and risk-free network infrastructure.

4.10.2. Policy Statements

The University shall:

a. Establish comprehensive and up-to-date ICT security risk assessment SOPs for identifying security vulnerabilities and threats posed to critical business information assets and ICT resources.
b. Enforce comprehensive and up-to-date ICT security standards for risk mitigation, to enhance confidentiality, integrity and availability of critical business information assets and ICT resources.
c. Form a Security Risk Assessment and Mitigation Team (SRAMT) that will be responsible for carrying out comprehensive risk assessment and analysis of critical business information assets and ICT resources. Also, the team shall be responsible for implementing security risks mitigation plans. Team functions and composition is to be established by CERT.

4.11. Principle XI: ICT Security Compliance and Audit, Monitoring, Disciplinary Measures, and Review Management

4.11.1. Aim

This principle aims to ensure that the University and its ICT users comply with security related regulatory and legal frameworks in Tanzania.

4.11.2. Policy Statements

The University shall:

a. Comply with relevant statutory, regulatory, and contractual requirements, and that the approaches to meet these requirements shall be explicitly identified, documented and kept up to date for each ICT product, facility and service
b. Ensure privacy and protection of personally identifiable information, in compliance with relevant laws and regulations.
c. Develop and implement rules and procedures to ensure compliance while implementing the UDSM ICT Security Policy. Any violation of the policy would attract appropriate penalties as defined in the rules and procedures.
d. Establish and enforce appropriate system audit mechanisms for monitoring, checking and enforcing compliance of security requirements. The mechanisms shall involve the use of automated tools to provide real time notifications about detected wrongdoing and vulnerabilities; such tools include intrusion detection, system logs, firewall logs, user account logs, network scanning logs, application logs, data backup and recovery logs, help desk logs, and error log files.
e. Develop compliance mechanisms for enforcing adherence to ICT security policy and standards, to ensure that no individual attempts to gain unauthorized access to ICT resources or intentionally damage, alter, or disrupt the operation of ICT resources. Failure to comply with the University policies and regulations and national laws shall lead to disciplinary measures.
f. Establish and enforce the usage of appropriate mechanisms for conducting periodic review of user and third-party agreements and contracts (SLAs/OLAs) to ensure that they comply with national laws and UDSM policies. In case of any violation, the findings shall be reported to appropriate authorities.
g. Establish and enforce usage of SOPs to handle any exceptional case that requires exemption from the security treatments defined in this policy.
h. Establish an ICT Security Policy Implementation and Review Team (SPIRT) to conduct annual review and update of this policy to cope with the dynamics of ICT security requirements. The review shall focus on such aspect as the assessment of security threats, establishing existing ICT resources and the associated security risks, security mitigation posture, and SLAs/OLAs.

5. ICT Security Policy Implementation Instruments

The implementation of this policy shall require development and enforcement of various policies, rules, regulations, or SOPs as circumstances shall require. In their totality, the documents are implementation instruments of this ICT Security Policy. The documents include but are not limited to the following:

a. ICT Security Strategy – to guide the implementation of UDICTSP;
b. ICT Security Guidelines and Procedures - provide procedural guidance to establish, manage, implement and maintain information security.
c. ICT Business Continuity and Disaster Recovery Plan (ICTBC & DRP).
d. Information Assets Classification and Control.
e. Human Resources Management.
f. ICT Security Awareness and Acceptable Use of ICT Resources.
g. Physical and Environmental Controls of ICT Resources.
h. Computer and Network Security Management.
i. Computer Passwords and System Access Controls.
j. Wireless Network, Mobile Computing and Tele-working.
k. Procurement and Contracts Management
l. Security Risk Assessment and Requirements for Information Assets.
m. Systems Development and Maintenance.

This policy and its implementation documents listed above shall be summarised in a non-technical language and posted on the DICT website for creating awareness and for quick reference by all users of the University information assets and ICT resources.

6. ICT Security Policy Implementation Teams

The implementation of this policy shall be coordinated by the Directorate of ICT (DICT), and shall require the formation of the following ICT security teams:

- Computer Emergence Response Team (CERT/ CSIRT)
- ICT Security Policy Implementation and Review Team (SPIRT)
- ICT Security Risk Assessment and Mitigation Team (SRAMT)

These teams shall work closely with teams identified in the UDSM ICTBC & DRP, based to the nature and urgency of security issues to be attended.

Bibliography

1. Building a Business continuity Plan, Guidelines for Preparation of Your Plan [Retrieved from: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/property-insights/business-continuity-planning-guidelines-for-preparation-of-your-plan.pdf, Last accessed January 2022]
2. ISO/IEC 27000 (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000:2018 (E)).
3. ISO-27K, ISO 27001: 2013 (2013). Code of practice for Information Security Risk Management. [Retrieved from: https://www.iso.org/standard/54534.html, last accessed February, 2022].
4. Karokola, G. (2012): *A Framework for Securing e-Government Services – The Case of Tanzania*. PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm/ Royal Institute of Technology (KTH), Stockholm, Sweden, ISBN: 978-91-7447-583-8.
5. TZ-eGA (2021). Disaster recovery guide *[Retrieved from:* https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.ega.go.tz%2Fuploads%2Fstandarddocuments%2Fen-1631189021-Disaster%2520Recovery%2520Plan%2520Sample_final.docx&wdOrigin=BROWSELINK, last accessed January 2022].
6. Tanzania eGA (2013). Tanzania e-Government Strategy. Tanzania e-Government Agency. Dar es Salaam. [Retrieved from: http://www.tanzania.go.tz/, last accessed January, 2022].
7. Tanzania eGA (2021). Technical Guideline for developing ICT Security Policy, [Retrieved from: https://www.ega.go.tz, last accessed February 2022].
8. MoWTC (2016). National Information and Communication Policy. Tanzania Ministry of Works, Transport and Communication. Dar es Salaam. [Retrieved from: http://www.tanzania.go.tz/, last accessed January, 2022].
9. Tanzania Vision 2025. Development Vision 2025 for Tanzania. The United Republic of Tanzania.
10. Tarimo, C. (2006). ICT Security Checklist for Developing Countries: A Social-Technical Approach. PhD Thesis, Department of Computer and Systems Sciences, University of Stockholm/ Royal Institute of Technology (KTH), Stockholm, Sweden, ISBN: 91-7155-340-1.
11. TCRA (2022). Tanzania Communication Regulatory Authority. [Retrieved from: http://www.tcra.go.tz, last access January 2022].
12. UDSM (2022). University of Dar es Salaam ICT Policy (2022 – 2027).
13. UDSM (2022). University of Dar es Salaam ICT Master Plan (2022 – 2032).
14. UDSM (2022). University of Dar es Salaam Business Continuity and Disaster Recovery Plan for ICT (2022 – 2027).
15. UDSM (2006). University of Dar es Salaam ICT Policy (2006 – 2010). University of Dar es Salaam.
16. UDSM (2016). University of Dar es Salaam ICT Security Policy (2016 – 2020)

17. UDSM (2008). The University of Dar es Salaam ICT Master Plan (2008 – 2012), University of Dar es Salaam.

18. UDSM (2061). University of Dar es Salaam Vision 2016. University of Dar es Salaam.

19. UDSM (2016). University of Dar es Salaam Risk Register. University of Dar es Salaam.

20. UDSM (2014). University of Dar es Salaam Corporate Strategic Plan (2014-2013). University of Dar es Salaam.