UNIVERSITY OF DAR ES SALAAM

Acceptable Use of ICT Resources Policy

Directorate of Information and
Communication Technologies

June 2024

Plan Approval

Document name	Acceptable Use of ICT Resources Policy
Version	UDSM/ICT/AUICTRP/V1.0_2024
Prepared by	Directorate of Information and Communication Technologies
Owned by	University of Dar es Salaam
Approved by	University Council
Date Approved	
Signature	
Signed by	

Document information

Document Name	Acceptable Use of ICT Resources Policy
Category	Security of Information and Communication Technology Resources
Related policies, standards and guidelines.	• UDSM ICT Policy • UDSM ICT Security Policy • UDSM Business Continuity and Disaster Recovery Plan • UDSM ICT Master Plan. • UDSM Information Assets Classification and Control Guideline
Version number	UDSM/ICT/AUICTRP/V1.0_2023
Approval date	
Approved by	University Council
Signature & Date	

Details of Version History and Authors

Version and Date	Reason for revision / change	Revised/Changed by
V1.0: 01/04/2024	*First Draft Document Submitted for Approval*	*DICT Team*

TABLE OF CONTENTS

ACRONYMS AND ABBRIVIATIONS

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

1. INTRODUCTION

This document formalizes the policy for employees, students, stakeholders and third parties ("users") of the University of Dar es Salaam (UDSM) on the information and communication technology (ICT) Acceptable Use of ICT Resources Policy (AUICTRP) which include computers, printers and other peripherals, computer programs, data, local area network, video conference facilities, door access control systems, CCTV, intranet and the Internet.

2. PURPOSE AND OBJECTIVES

This Policy enables users to understand ICT security awareness as well as what is considered acceptable and unacceptable in the use of UDSM ICT resources. It sets out the required behaviours and actions when using UDSM ICT equipment, network infrastructure, application and system software and ICT services, including incidental personal use of ICT systems, email addresses and the Internet. The main purpose of this document is to set out how relevant stakeholders shall adhere to UDSM policy on AUICTRP. More specifically, the objectives of this policy are to:

i. ensure that UDSM ICT resources are used appropriately and responsibly.

ii. ensure that appropriate password controls are implemented to address the risk of unauthorised access to the UDSM ICT resources.

iii. safeguard the integrity and security of UDSM ICT facilities and services; and

iv. ensure common and consistent understanding of UDSM staff members responsibilities when using electronic messaging services.

3. SCOPE

This policy applies equally to all UDSM employees, students, including permanent, temporary, part-time and contract employees, as well as contractors, consultants, or any other third parties who use ICT resources owned, leased, or rented by UDSM and includes use at home. It also applies to any person connecting personally owned equipment to the UDSM network infrastructure from any location.

4. THE POLICY STATEMENTS

The AUICTRP statements are categorised into 13 sections which are: ICT and Cyber Security Awareness; Acceptable Behaviour; Unacceptable Behaviour; Acceptable use of ICT Resources; Managing online presence and social media usage; Acceptable Email Use; Internet and Intranet Usage; Use of Passwords, Password security and Authentication; Security of UDSM ICT Facilities/ Equipment; Portable and Mobile Devises Usage; Closed Circuit Television (CCTV) Usage and Software Use and Licensing.

4.1. ICT and Cyber Security Awareness

4.1.1. UDSM shall on a regular basis conduct awareness training programmes on the ICT and ICT security issues to all employees, students and other stakeholders.

4.1.2. UDSM shall ensure all employees and stakeholders are:

i. aware of their responsibility when accessing UDSM data.

ii. being issued with the relevant policies and guidelines on acceptable use of ICT resources.

iii. keeping all related data secure including all personal, sensitive, confidential or classified data.

iv. responsible to ensure the security of any personal, sensitive, confidential and classified information contained in faxed, copied, scanned or printed format, particularly, when shared multi-function printers, fax machines, scanners and copiers are used.

4.1.3. UDSM is committed to complying with legal requirements and internationally recognised information security best practices. These shall include secure creation, sharing, storing and destructing information in all its forms. ICT security of an institution is governed by the following key components:

i. People

a. Business requirements and objectives remain at the core of ICT security provision;

b. Work with individuals and services to minimise and reduce risk and recommend secure solutions;

c. Record and report ICT security-related metrics and make them available on the core;

d. A consistent information security awareness programme will contribute to a strong ICT security culture.

ii. Process

a. Information will be protected against unauthorised access and misuse.

b. ICT business continuity and disaster recovery plans will be maintained and regularly tested.

c. Policies, standards, processes and guidelines will be regularly reviewed and updated as necessary.

d. Information security incidents such as breaches, threats, weaknesses or malfunctions will be recorded and investigated using a formal process.

e. Assets and information will be classified and protected according to classification criteria.

iii. Technology

a. ICT will work to continuously improve using automated processes.

b. *Changes to ICT systems, solutions and technologies at UDSM will be improved and carefully controlled prior to implementation.*

c. *Regular impact and vulnerability assessments will provide a clear understanding of gaps to be addressed;*

d. *UDSM will manage the security of UDSM ICT resources that provide 24/7 monitoring*

e. *UDSM will manage Network Operating Centre (NOC) that provide 24/7 monitoring of ICT network resources.*

4.2. Acceptable Behaviour

Proper use of ICT resources empowers users by make their jobs and other activities more fulfilling by allowing them to deliver better services. Thus, UDSM employees and stakeholders are encouraged to optimally use ICT resources in pursuit of UDSM's goals and objectives.

4.3. Unacceptable Behaviour

4.3.1. Create, display, produce, download or circulate offensive materials in any form or medium as stipulated by the laws of the land.

4.3.2. Failure to adhere to the terms and conditions of all license agreements relating to ICT facilities used including software, equipment, services documentation and other goods.

4.3.3. Deliberately introducing viruses, worms, trojan horses or other harmful or nuisance programs or files into any UDSM ICT resources, or taking deliberate action to circumvent any precautions taken or prescribed by the institution.

4.3.4. Loading onto the UDSM ICT facilities any software without permission from DICT.

4.3.5. Moving or relocating ICT facilities belonging to or used by another user without consent.

4.3.6. Failure to report any observed or suspected security incidents, weaknesses, or threats.

4.3.7. Allow non-UDSM employee and non-approved stakeholders to use ICT resources assigned to him/her without prior authorization.

4.3.8. Users shall not upload any business files to personal Internet sites or via personal email/social media as they put the data out of UDSM control and may result in leakage of confidential information.

4.3.9. Use any UDSM ICT facilities for any personal activities that are prohibited under the law.

4.3.10. It is unacceptable for any person to use UDSM ICT resources:

i. in furtherance of any illegal act, including violation of any criminal or civil laws or regulations;

ii. for any political purpose;

iii. for any personal commercial purpose;

iv. to send threatening or harassing messages

v. to access or share sexually explicit, obscene, or other inappropriate materials;

vi. to infringe any intellectual property rights;

vii. to gain, or attempt to gain, unauthorized access to any device or network;

viii. to cause interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs;

ix. to intercept communications intended for other persons;

x. to misrepresent either UDSM or a person's role at UDSM;

xi. to distribute chain letters or messages;

xii. to access online gambling sites; or

xiii. to negatively label or otherwise defame any person.

4.4. Acceptable use of ICT Resources

4.4.1. Users shall not disclose, or disseminate to unauthorized person, any information or data that they come across when using UDSM ICT resources.

4.4.2. Users shall only access or try to access information they are granted access to.

4.4.3. Users shall ensure that any discarded information or data is properly disposed off.

4.4.4. Users shall not disclose any proprietary or confidential information about UDSM and/ or its clients, including client contract information, internal policies, standards, procedures, processes, guidelines or financial information through emails, messages, social media postings, blogs, or any other means.

4.4.5. Users shall not breach the rights to data privacy, that shall adversely affect UDSM reputation through comments or postings made regarding other individuals.

4.4.6. Users shall not accept offers of software upgrades or security patches from pop-up windows that appear when browsing the Internet, as these often contain malware.

4.4.7. The University shall not be responsible to provide ICT support or backup arrangements for personal applications and downloads, or any support to help manage employee personal files.

4.4.8. Users shall remove any downloaded software, music or other data, which is for personal use, that is found or suspected to interfere with the performance of UDSM network (UDSMNet) or is inappropriately licensed from the computer owned by UDSM.

4.4.9. All users shall be given awareness training on the acceptable use of the UDSM ICT assets by the UDSM Directorate of ICT.

4.4.10. It is the responsibility of all UDSM employees, students and other users of UDSM ICT resources to ensure the following:

i. immediately switch off a computer screen or close a window with inappropriate content and report the incident immediately to the UDSM ICT support team.

ii. report to the ICT support team when they identify that the computers, they use, do not have anti-virus protection or the anti-virus protection is not up to date.

iii. Personal computers connected to UDSM network have anti-virus protection.

4.5. Managing online presence and social media usage

4.5.1. UDSM offers access to social networking sites to employees and stakeholders via the UDSM network.

4.5.2. Users to set and maintain the maximum privacy possible on online platforms and deny access to unknown individuals.

4.5.3. Users are advised to be cautious about the information given online by others and that they should not trust every online account as being genuine.

4.5.4. Users to avoid placing images of themselves online or details within images that could disclose personal information not meant for public use.

4.5.5. Users to consider the appropriateness of any images they post online due to the difficulty of removing images once made available in the digital space.

4.5.6. Users to avoid giving out personal details online which may identify them or their location such as full name, address, mobile number, home phone numbers and family.

4.6. Acceptable Email Use

4.6.1. Users shall not use their work email address *(@udsm.ac.tz domain or sub-domains)* for any non-work purposes that may reasonably be mistaken as being related to UDSM, e.g., correspondence with the media, registering domain names or ordering the supply of business-type goods (even if this is for delivery to your home address).

4.6.2. UDSM shall reserve the right to inspect, monitor and disclose the contents of any email created, sent, received, or forwarded by using its network or email system.

4.6.3. Emails addressed to other institutions or individuals outside UDSM shall clearly identify the sender by full name, position and contact address.

4.6.4. Users shall ensure that the content and tone of their e-mail messages cannot be considered offensive or abusive or of a discriminatory or bullying nature or constituting harassment of any kind.

4.6.5. UDSM employees, students and other users of UDSM ICT resources shall not send chain emails addressed to larger user groups without approval.

4.6.6. Users shall be careful when opening email attachments received from unsolicited or mistrusted senders, as this may contain malicious codes.

4.6.7. UDSM employees, students and other users of UDSM ICT resources shall be responsible for the content of emails sent from their email addresses.

4.6.8. Users of UDSM ICT resources shall not spoof or otherwise falsify a sender address.

4.6.9. UDSM employees, students and other users of UDSM ICT resources are not authorised to access to another employee's data files and emails without the consent of the latter.

4.6.10. Users must not send electronic mail that contains ethnic slurs, racial epithets, or anything that may be construed as harassment or criticism of others based on their race, national origin, sex, age, disability, religion, or political beliefs.

4.6.11. Users shall not use their email to distribute, disseminate or store images, text or materials that might be considered indecent, pornographic, or illegal.

4.6.12. Users shall not knowingly or purposely send emails containing computer viruses, worms, trojan horses, or any other form of malware that could damage or interfere with the UDSM ICT network or another user's devices.

4.6.13. UDSM employees, students and other users of UDSM ICT resources shall not send unapproved chain letters, spam emails, or pyramid emails to anyone at any time.

4.6.14. UDSM employees, students and other users of UDSM ICT resources shall refrain from sending broadcast emails: sending the same message to a large number of recipients unless necessary.

4.6.15. Users shall avoid sending excessively large electronic mail messages or attachments.

4.6.16. Users shall double-check the email addresses of recipients when forwarding email messages.

4.6.17. Students' email addresses will be deactivated six months after graduation dates.

4.6.18. Email addresses of UDSM staff who leave the university for any reason will immediately be deactivated.

4.6.19. Staff and students whose email addresses are to be deactivated but might need to continue using UDSM email addresses for some official purposes may request access from UDSM management.

4.7. Internet and Intranet Use

4.7.1. Internet access through UDSMNet shall be provided to authorised users only.

4.7.2. Users shall not use the Internet to transmit any proprietary, confidential, or otherwise sensitive information unless it is necessary and if so, take proper security control measures as advised by ICT team.

4.7.3. Unless specifically authorized, on an item-by-item basis, users are strictly prohibited from using the Internet to:

i. Download games or shareware programs.

ii. Play games or participate in any online contest or promotion.

iii. Disable or overload any computer system or network or attempt to disable, defeat, or circumvent any system intended to protect the privacy or security of another user.

iv. Download or distribute pirated software or restricted data in the UDSMNet infrastructure.

4.7.4. All official internal publications shall be posted on the Intranet once approved by the appropriate UDSM data custodian or steward.

4.7.5. The use of the Intranet is intended exclusively for the work undertaken for or by UDSM.

4.7.6. Sensitive or confidential information shall not be exchanged via the Intranet.

4.7.7. Users shall act responsibly and maintain the integrity of the data or information within the Intranet at all the times.

4.7.8. All information or data posted to the Intranet shall be checked for viruses or bugs.

4.7.9. Internet usage activities of UDSM employees, students and other users of UDSM ICT resources may be monitored by the DICT.

4.7.10. Users shall protect their login credentials, such as user IDs and passwords and shall in no case be shared with colleagues or with anyone else.

4.7.11. Personal user credentials, such as user IDs and passwords shall not be stored on Internet browsers or stored in computer files, written on paper, or written anywhere visible.

4.7.12. UDSM is responsible to recognise and register all personal devices eligible to connect to UDSMNet.

4.7.13. Users shall not connect any personal devices on their workstations to access the UDSM Internet directly, except when authorised by DICT.

4.7.14. UDSM employees, students and other users of UDSM ICT resources shall not access UDSM confidential data via private or public devices.

4.7.15. It is strictly prohibited to download unapproved software using UDSMNet and install the same on UDSM ICT devices or personal devices used on UDSMNet.

4.7.16. Users shall not use UDSMNet to download movies, pictures and music files unless work-related.

4.7.17. All downloaded files from the Internet shall be scanned using dependable anti-virus before they can be used on UDSM ICT devices.

4.7.18. Users shall not deliberately try to bypass security controls on UDSM systems to access the Internet.

4.7.19. Users shall not be allowed to disable the anti-virus protection running on their computers for browsing the Internet.

4.7.20. Users must not use the Internet provided at work to gain unauthorised access to other systems or websites.

4.7.21. Users shall be forbidden from using file-sharing technologies, except those recommended by the ICT office (DICT).

4.7.22. Users of UDSM owned portable devices accessing the Internet from public places shall make sure that proper security measures are maintained and shall not connect to an unsecured network.

4.8. Use of Passwords, Password Security and Authentication

4.8.1. UDSM ICT Resources shall be accessed through secret-based (e.g., usernames or user IDs and passwords or PINs) or biometric authentication methods (e.g., fingerprint, facial recognition).

4.8.2. User department must notify DICT of any change of staff or student status made which may affect their access rights to use UDSM ICT facilities.

4.8.3. Computer users shall create system passwords that are a minimum of eight (8) characters in length and must be, to the extent possible, comprised of letters, numbers, upper and lower cases and special characters.

4.8.4. Users of UDSM ICT resources shall be required to;

i. avoid using another user's username and password, or allow passwords issued to them to become known to any other person.

ii. avoid leaving ICT facilities unattended after logging in.

iii. ensure their passwords are not based on personal information like family names, birth date, login name or common words and phrases.

4.8.5. All users shall change their passwords whenever there is any indication of possible system or password compromise.

- Users should be aware that all dormant user accounts are disabled after thirty (30) days of inactivity (excluding administrators).

4.8.6. Users should be aware that prompt action will be taken to disable accounts of users who lose their authorised access rights, have left the university, have died, or those whose access rights are changed based on changing responsibilities.

4.8.7. Initial passwords that have been assigned as original user passwords shall be changed at the first user log-on, whether the information system forces the change or not.

4.8.8. Users shall log off from their connection session every time they complete tasks.

4.8.9. Personal computers, laptops and servers shall have password-protected screen savers.

4.8.10. Password-protected screen-savers shall be automatically activated at most after three (3) minutes.

4.8.11. When not turned off, PCs and terminals shall be protected from unauthorised use by appropriate controls such as key-lock or BIOS password.

4.8.12. Users must be aware that UDSM systems enforce them to change passwords after every sixty (60) days for critical systems and ninety (90) days for all other systems.

4.8.13. Users should avoid making their passwords visibly displayed while typing.

4.8.14. Users should be aware that they will be locked out of the system they are attempting to access upon three (3) consecutive authentication failures and must follow the provided security procedures for resetting passwords.

4.8.15. Users should be aware that connection sessions that are not active for more than thirty (30) minutes shall automatically terminate both for the application and network sessions.

4.9. Security of UDSM ICT Facilities and Equipment

4.9.1. Users shall be responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use.

4.9.2. No equipment or other ICT facility shall be moved from its location without the prior agreement of the designated authority.

4.9.3. No equipment may be connected in any way into the UDSMNet infrastructure or other ICT facility without authorisation from DICT.

4.9.4. User shall immediately notify the ICT team about missing or stolen equipment through phone calls, email, or face-to-face.

4.9.5. When ICT equipment is stolen, it shall first be reported to the Police then other internal reporting processes will continue.

4.9.6. Users shall avoid taking any food or drink close to ICT equipment and into computer laboratories.

4.9.7. Equipment shall be switched off properly before leaving the office or computer laboratories.

4.9.8. Users are not allowed to alter any hardware or software installed in UDSM computers or other computing devices.

4.9.9. Any equipment or media taken off UDSM premises shall not be left unattended in a public place.

4.9.10. Users of UDSM portable devices such as laptops, tablets and removable media are responsible for ensuring that proper physical handling is maintained and keeping visual control over them at all times. Laptops and tablets should be carried as hand luggage and disguised where possible when travelling and shall not be left in cars unattended.

4.9.11. Users of UDSM ICT equipment in public areas shall take proper safeguard to ensure that unauthorised viewing of confidential or restricted data is avoided by attending their devices at all times or locking device screens when not in use.

4.9.12. Laptops, tablets and smartphones containing university-related confidential information shall be protected with an appropriate form of access protection to prevent unauthorised access by using passwords, smart cards, fingerprint, encryption, or any other appropriate means.

4.10. Portable and Mobile Devices Usage

4.10.1. Mobile devices authorised to connect to the UDSMNet infrastructure shall adhere to the following policies:

i. Their operating systems and any installed software must be kept up to date.

ii. They must be installed with up-to-date antivirus and antispyware to provide protection from viruses, worms, trojan horses, disruptive programs, or devices or anything else designed to interfere with, interrupt or disrupt the normal operating procedures of UDSMNet.

iii. A personal firewall may be installed to provide protection from unauthorized intrusions.

iv. They must not have a blank password and all default passwords shall be changed.

4.10.2. All mobile devices (such as laptops, mobile phones and tablets) supplied by UDSM shall remain the property of UDSM and usage of the same shall therefore be monitored and audited.

4.10.3. Employees shall take appropriate measures to protect UDSM mobile devices against accidental loss, damage, or theft.

4.10.4. Employees shall immediately inform the DICT office, after reporting to the police, when a UDSM device is stolen or lost to prevent unauthorised access to confidential information.

4.10.5. Users of UDSM mobile devices shall contact the DICT office for the installation of software applications on their devices.

4.10.6. Passwords for access to core UDSMNet infrastructure and systems shall not be stored on mobile devices.

4.10.7. Any UDSM mobile device no longer used by the user, whether functional or damaged, must be returned to the DICT office**.**

4.11. Closed Circuit Television (CCTV) Usage

4.11.1. The management of the CCTV system shall be the responsibility of the DICT office.

4.11.2. Users should be aware that access to the CCTV Control Room is granted only to staff or visitors on a case-by-case basis after a written authorisation by DICT.

4.11.3. Users should be aware that materials or knowledge secured as a result of the use of CCTV systems shall not be used for any commercial purposes.

4.11.4. Users should be aware that any CCTV recorded data shall only be released for use in the investigation of a specific crime and with the written authorisation.

4.11.5. Users should be aware that any complaints about UDSM's CCTV system should be addressed to the DICT office.

4.11.6. Users should be aware that all CCTV feeds are backed up and stored for a period of 90 days depending on the classifications and sensitivity of the feeds.

4.12. Software Use and Licensing

4.12.1. Only licensed software may be used to perform UDSM businesses.

4.12.2. Any software installed on UDSM ICT facilities for incidental personal use must be licensed.

4.12.3. UDSM’s ICT resources or networks must not be used to acquire, copy, or distribute software, or other copyrighted material without appropriate licenses.

4.12.4. UDSM shall retain the rights to applications and source codes developed during working hours on UDSM's ICT facilities. This includes ICT applications developed for UDSM, developed externally or paid for by UDSM.

4.12.5. Users shall not install UDSM’s licensed applications and software for use on non-UDSM ICT facilities without authorisation.

4.12.6. Users should be aware that software, service or media files found to interfere with the normal operation of UDSM systems or are considered to pose an unacceptable risk shall be removed.

4.12.7. Users should be aware that periodic scans of all PCs and mobile devices connected to UDSM network are performed by DICT to identify devices that pose threats.

4.12.8. Users should be aware that software applications installed in UDSM computers or personal user computers that are no longer needed shall be uninstalled so that the license can be made available for reassignment.

5. IMPLEMENTATION, REVIEWS AND ENFORCEMENT

5.1. Implementation and Reviews

5.1.1. This document shall come into operation once approved by the UDSM ICT Steering Committee and then shall be considered mandatory for all UDSM business operations.

5.1.2. Failure to observe this policy may subject individuals to loss of access privileges to UDSM ICT resources or to disciplinary action which may include termination of employment or contract or a criminal case.

5.1.3. This document shall be reviewed after three years or at any time whenever the UDSM business environment changes in a way that affects the current policy or the need to improve any aspect of this policy arise.

5.2. Roles and Responsibilities

5.2.1. It is the responsibility of any person using UDSM's ICT resources to read, understand sign and follow this policy.

5.2.2. Users are expected to exercise reasonable judgement in interpreting this policy and in making decisions about the use of ICT resources.

5.2.3. Any person with questions regarding the application or meaning of statements in this policy shall seek clarification from the DICT office.

5.2.4. DICT shall enforce compliance by using audit trails and trigger access revocation or removal to UDSM systems and networks.

5.3. Monitoring and Evaluation

5.3.1. The UDSM ICT Steering Committee shall, as part of its meetings' agenda, monitor and evaluate the implementation of this policy.

5.3.2. DICT shall conduct regular assessments to establish the need for improving this policy or accommodating new requirements in response to the new development of UDSM ICT resources and the users.

5.4. Exceptions

In case of any exceptions to this policy, it shall be thoroughly documented and followed through a proper channel of authorisation using the same authority which approved this document.

6. APPENDIX

6.1. Appendix I - Declarations by UDSM Staff, Students, Contractors and other Third-Party Users.

These declarations have been designed to certify that users of UDSM ICT resources acknowledge that they are aware of UDSM Acceptable Use of ICT Resources Policy and agree to abide by their terms.

I ……………………………………………………………………..…. acknowledge that the **UDSM** Acceptable Use of ICT Resources Policy has been made available to me for adequate review and understanding. I certify that I have been given ample opportunity to read and understand it and ask questions about my responsibilities on it. I am, therefore, aware that I am accountable to all its terms and requirements; and that I shall abide by them. I also understand that failure to abide by the terms and requirements of this policy grants **UDSM** the right to take appropriate disciplinary or legal action, or both, as the case may be.

Signature:……………………………………………

Department/Unit:……………………………………..
Job Title:………………………………………………..

Date: ____ / __ / ____

6.2. Appendix II – Definitions of Key Terms and Concepts

Accountability – When a specific action is associated with an individual.

Anti-malware Software – Software installed on a computing device that protects it from malicious software.

Application – a software program or group of software programs designed to work together to accomplish specific business objectives.

Approved software – Software that has been reviewed and deemed acceptable by the Authority for use with its ICT resources

Asset Custodian - the nominated individual who has responsibility for the security of the data and application component of the Information Asset and is also accountable for those aspects of the Information System.

Audit logs – Documentation of activity incorporating, at the minimum, date, time, action and account details.

Authentication – the process of confirming that a known individual is correctly associated with a given electronic credential, for example, by use of passwords to confirm correct association with a user or account name.

Authorization – the process of determining whether or not an identified individual or class has been granted access rights to an information resource and determining what type of access is allowed, e.g., read-only, create, delete and/or modify.

Business System - any Information System which 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.

Confidential Information and/or Confidential Data – Information/Data that are exempted from disclosure under the provisions of applicable state and federal law.

Critical Information Resources – the resources determined by the management to be essential to its critical mission and functions, the loss of which would have an unacceptable impact.

Data store – A collection of information organized so it can be accessed, managed and updated.

Hardware Failure – refers to the failure of ICT equipment such as a computer, its storage devices, or the computer network

ICT/ IT - any communication device or application, including: radio, television, cellular phones, computer and network hardware and software, satellite systems and associated services and applications.

ICT Security Policy – a document that articulate a high-level statement of organizational beliefs, goals and objectives and the general means for their attainment in a specified subject area.

Security - preservation of:

- **Confidentiality**: ensuring that information is accessible only to those authorized to have access;
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods; and
- **Availability:** ensuring that authorized 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 or contractors - persons who use ICT assets to provide services to University Users, whether they are located on the University campus or otherwise.

Users of UDSM ICT resources include but are not limited to:

- All Students and University Staff;
- Other persons and organizations 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 persons using the University's ICT Assets to do business with the University, whether as a researcher, contractor, consultant or supplier.

Information Asset - all significant software, hardware and data used in the management of the related University information resources or the general operations of the university.

Information Security – refers to the preservation of Confidentiality – protecting information from unauthorized access and disclosure; Integrity – safeguarding the accuracy and completeness of information and processing methods; and Availability – ensuring that information and associated services are available to authorized users when required.

Information Security Classification - categorisation of an Information Asset for the purposes of identifying the security controls required to protect that asset.

IT Infrastructure - Network devices, server hardware and host operating systems.

IT Resources – Refers to computer hardware, software, networks, devices, connections, applications and data.

Least Privilege – The principle that grants the minimum possible privileges to permit a legitimate action, in order to enhance protection of data and functionality from faults and malicious behaviour

Malware – Malicious software

Mobile Computing Device – A laptop, PDA, or other portable device that can process data

Peer to Peer – Communications model that allows the direct sharing of files (audio, video, data and software) among computers.

Remote Access – Any access to an agency's 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 the system 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 to apply 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 applying 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 required to complete a task. This 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, shall be considered.

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 list of configurations, software or hardware

Visitor - any person who accesses an ICT system, service or equipment owned, managed or supplied by UDSM or one of its partners, but is not a UDSM student or member of staff.