KIAMBATISHO 237.4.9

UNIVERSITY OF DAR ES SALAAM

ICT SECURITY POLICY

2016 – 2020

June 2016

Table of Contents

List of Abbreviations and Acronyms

BCP	Business Continuity Planning
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CSIRT/CERT	Computer Security Incident/Emergency Response Team
DRP	Disaster Recovery Planning
EKM	Encryption Key Management
Email	Electronic Mail
ICT	Information and Communications Technology
IS	Information System
ISC	Information Security Classification
ISIRT	ICT Security Incident Response Team
ISO	International Standards Organisation
ISP	ICT Security Plan
IT	Information Technology
LAN	Local Area Network
OLA	Operational Level Agreement
PCs	Personal Computers
OLA	Operation Level Agreement
SLA	Service Level Agreement
SRAMT	Security Risk Assessment and Mitigation Team
UPS	Uninterruptible Power Supply
WAN	Wide Area Network
WLAN	Wireless LAN
UDSM	University of Dar es Salaam

1. Introduction

The University of Dar es Salaam (UDSM) has over time invested in Information and Communication Technology (ICT) infrastructure in an effort to improve its administrative, teaching, learning and research functions. The University has procured and implemented at various locations, ICTs that are used to create, process, store, share and disseminate data and information. This infrastructure is used to run different systems and applications which hold vital information. All these are assets which represent a significant economic investment by UDSM. Their continued availability in support of the UDSM core business functions is of utmost importance, hence, there is a need to secure and control their access.

The University recognizes that ICT security is an issue for the whole University community, if it is to benefit from its ICT investments since the technology can enable rapid spread of attacks and exploits, which can undermine the success of the University. The University has therefore decided to introduce this policy in order to manage the risks associated with ICT.

This document therefore defines the UDSM ICT Security Policy for ICT assets. The ICT assets including information provided for academic purposes and University business are extremely valuable for the day to day delivery of University services. This policy is designed to support all areas of the University's business and to recognise academic freedoms when using ICT assets. The intention is that this ICT security policy will enable the University to carry out its activities, by protecting and preserving University ICT assets at the appropriate level of security controls. The policy is intended to protect the ICT assets of the University by adopting the core principles of information security namely Confidentiality, Integrity and Availability.

Therefore the implementation of this ICT Security Policy will necessitate the development and enforcement of various rules, procedures, and standards, which must be followed by all users who are given access to the University's critical business information assets and the associated ICT resources. The main purpose of the ICT security policy and the rules, procedures, and standards for its enforcement is to guide and inform users of the requirements and their obligations in protecting UDSM's ICT resources and information assets.

2. Purpose

The University of Dar es Salaam is to adopt the ICT Security Policy described hereunder as a means of protecting the confidentiality, integrity and availability (CIA) of institutional data as well as any information systems that store, process or transmit institutional data. This Policy applies to all Users of UDSM critical business information assets and the associated ICT resources.

3. Audience

This policy is intended for all users of ICT equipment, services and information within the University of Dar es Salaam. Categories of users in this policy includes, but not limited to: Students enrolled at the University, permanent staff employed by the University; temporary, casual or agency staff working for, or on behalf of the

University; contractors, consultants and suppliers working for, or on behalf of the University; visitors to the University and collaborative partner institutions who have access to UDSM ICT systems and services.

4. Scope

This policy applies to all of the University's electronically stored data and ICT assets and all users both on-campus and at other locations worldwide including but not limited to:

a) The Network and related network services including networks with wired, wireless, dialup and/or Internet connections;

b) Computers and related peripherals including servers, desktop PCs, laptop, printers, copiers, scanners, removable media and mobile devices;

c) Information systems including the Academic Registry Information System, Library Information system, Financial Information System, University databases, Learning management systems, e-mail systems; and

d) Any other system that may be installed to provide a service on the University network.

5. Definitions

The terms "*University of Dar es Salaam*", "University" or "*UDSM*" will refer to University of Dar es Salaam and its constitute Colleges and Schools.

The term "*Policy*" would mean UDSM ICT Security Policy. Policy is defined as a high-level statement of organizational beliefs, goals, and objectives and the general means for their attainment in a specified subject area.

The term "*ICT*" refers to any communication device or application, including: radio, television, cellular phones, computer and network hardware and software, satellite systems and associated services and applications.

The term "*visitor*" refers to 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.

Security is the 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

Students includes currently registered students (including visiting students), as well as prospective, and former students of the University.

University staff or employee includes permanent and temporary academic staff, academic visitors and permanent and temporary administrative and/or technical staff (including persons on any type of placement or work experience assignment).

Service providers or contractors are persons who use ICT assets to provide services to University Users, whether they are located on the University campus or otherwise.

Users of ICT include but are not limited to:

a) All Students and University Staff;

b) Other persons and organizations working with or on behalf of the University;

c) 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;

d) Any other person accessing or attempting to access any University ICT Asset to which public access has been provided; and

e) Any other persons using the University's ICT Assets to do business with the University, whether as a researcher, contractor, consultant or supplier.

Asset Custodian means the nominated individual that 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.

Business System means 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.

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

6. Principles

To effectively and appropriately achieve Confidentiality, integrity and availability (CIA) to UDSM critical information assets and ICT resources – the security control principles along with best practices security control elements were adapted from ISO 27000 series of standards. The principles were aligned to match with UDSM ICT environment. Additionally, based on the principles, the University critical issues were identified and their respective objectives were critically analysed and developed. Further, policy statements for mitigating the same were formulated accordingly. The following sections provide description of the security control principles:

6.1 Policy, Planning and Governance

6.1.1 Issues

The effective planning and governance of information assets and supporting systems is fundamental to services delivery, provision of integrated services and sharing of information. When undertaking information assets resource strategic planning, the University will ensure that the objectives are aligned with and directly support high-level organisational goals, objectives and business strategies and are consistent with relevant requirements.

6.1.2 Objectives

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

6.1.3 Policy Statements

a) The University shall develop an ICT Security Plan (ISP), ensuring alignment with the University business planning, general security plan and risk assessment findings;

b) The University shall 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 as required;

c) The University shall establish and document information security internal governance arrangements including roles and responsibilities to implement, maintain and control the operations of information security within the University;

d) The University shall establish and document information security external governance arrangements 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.

6.2 Assets Management Security

6.2.1 Issues

The University encourages sharing of information assets to ensure organisational effectiveness. Users of University's information asset are provided with access to University information in order to effectively carry out their activities. However, where there are confidentiality or privacy requirements, access is restricted to particular users' positions or organisational units according to business requirements. Therefore, each information system requires its own level of security based on its Information Security Classification (ISC). Each information system needs to be uniquely identified and assigned an Asset Custodian.

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

a) **Public** – information of a nature which does not warrant any restrictions on access from the community at large (e.g. website);

b) **Internal** – information which relates to University activities and which is of relevance in terms of application to or use by all members of the University community;

c) **Restricted** – information generated or utilized in the operation of University functions or business activities which require restrictions based on functional need, institutional risks and legislative requirements.

6.2.2 Objectives

The objectives of the Asset Management security control principle are: To ensure that all University information is assessed to determine its sensitivity and importance; and to ensure that all information assets are provided with the appropriate control and protection.

6.2.3 Policy Statements

a) All University information shall be given an Information Security Classification so that it can be managed and secured in a manner appropriate with its sensitivity and importance;

b) Each University Information System shall be uniquely identified and assigned an Asset Custodian as per the *Information Security Classification Policy and Procedures;*

c) When University information is created the creator shall determine the classification of that document based upon the confidentiality, sensitivity and criticality of the information. The Information Security Classification must be one of the classifications specified in the *Information Security Classification Policy and Procedures;*

d) All information assets shall be inventoried and custodians shall be identified to be held accountable for their security. 'Acceptable use' policies should be defined, and assets should be returned and access rights revoked when people leave the University;

e) Information on storage media shall be managed, controlled, moved and disposed of in such a way that the information content is not disclosed.

6.3 Human Resource Security

6.3.1 Issues

The University employees will be involved in the management, operation and use of various information assets and ICT resources. The University shall implement measures to minimize the risk of loss or misuse of information assets by ensuring that security controls are incorporated into University human resource management, including the development of supporting policies and processes. Security responsibilities shall be taken into account when recruiting permanent employees, contractors and temporary staff through adequate job descriptions and screening and included in contracts as terms and conditions of employment and other signed agreements on security roles and responsibilities. Employees and contractors need to be made aware of and motivated to comply with their information security obligations. Security aspects of a person's exit from the University or significant changes of roles should be managed, such as returning information assets in their possession to the designated UDSM officials and updating their access rights.

6.3.2 Objectives

The objective of this control 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 Universities' information assets.

6.3.3 Policy Statements

a) The University shall conduct induction and on-going training and security awareness programs, to ensure that all users of University's information assets are aware of and acknowledge the University's information security policy, their security responsibilities and associated security processes;
b) The University shall document and assign security roles and responsibilities where employees have access to security classified information or perform specific security related roles;
c) The University shall ensure that security requirements are addressed, in recruitment and selection and in job descriptions;
d) The University shall develop and implement procedures for the scrutinization of employee movement from, or within, the University to ensure that all ICT assets are returned and removal or withdraw of all access rights in accordance with the set regulations and terms of service.

6.4 Physical and Environmental Management Security

6.4.1 Issues

The University is facing a number of security issues related to physical and environmental management these includes physical access control and monitoring, equipment control, and environmental management of ICT facilities to be disposed.

6.4.2 Objectives

The main objective of this principle is to prevent unauthorized access, damage and interference to UDSM's business premises, business information assets, and ICT facilities. Also, to take precautions against disposition of ICT facilities as some are toxic when exposed to the environment such as sunlight and moisture.

6.4.3 Policy Statements

a) The University critical or sensitive business information processing facilities shall be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They shall be physically protected from unauthorized access, damage and interference.

b) *The University shall develop and implement standard procedures to enforce Physical access control.* The security perimeter shall be clearly defined. The perimeter of a building or site containing critical information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or 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) *The University shall establish standard procedures for Physical access monitoring* and manned reception area or other means to control physical access to the site or building housing Critical ICT assets. Access to sites and buildings shall be restricted to authorized personnel only;

d) *The University shall establish standard procedures for equipment security control*. Physical barriers shall, if necessary, be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding. Equipment shall be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage;

e) *The University shall establish standard procedures for environmental control management*. This shall include procedures for sanitization of ICT facilities prior to re-assignment or disposal in an environment friendly manner. However, special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

6.5 Communication and Operational Management Security

6.5.1 Issues

The University needs to effectively control all sources of communication and operations in the computing and network infrastructure. Failure to that may lead to security breaches.

6.5.2 Objectives

Objective of this principle is to ensure correct and secure operation of information processing facilities.

6.5.3 Policy Statements

a) The University shall establish procedures for managing and operating all information processing facilities. This includes the development of appropriate operating instructions and incident response procedures;

b) The University shall implement 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 changes must be authorized by the management or responsible authority. It will specify the instructions on:

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;

c) The University shall develop and implement procedures for system housekeeping activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, computer room and mail handling management and safety.

d) The University shall develop and implement operational programs for change management control, such as audit log management and audit trails. Also, 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 persons, and identifying responsibilities for aborting and recovering from unsuccessful changes.

e) The University shall develop and implement procedures to govern separation of duties between development and operational facilities as it may pose potential security exposures, including possibility of compromise, damage, or loss of data at the contractor's site. Risks shall be identified in advance, and appropriate controls measures shall be articulated with the said contract (SLA).

6.6 Access Control Management

6.6.1 Issues

Access to information, and business processes should be controlled on the basis of business and security requirements. This should take into account the policies for information dissemination and authorization.

6.6.2 Objectives

The University needs to adequately control access to its critical business information assets and ICT resources.

6.6.3 Policy Statements

a) The University shall develop, and maintain policy to govern access control mechanisms to suit UDSM business processes, functions and requirements. The policy shall cover access control rules and rights for each user or group of users, including security requirements of individual business applications, identification of all information related to the business applications, policies for information dissemination and authorization, consistency between the access control and information classification policies of different systems and networks, and relevant legislation and any contractual obligations regarding protection of access to data or services;

b) The University shall enforce user access control and privilege management. In addition, formal procedures shall be 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 the initial registration of new users to the final de-registration of users who no longer require access to business information assets and other ICT resources. In addition, UDSM shall conduct a formal process at regular intervals to review users' access rights;

c) The University shall enforce user responsibilities access control mechanisms to prevent unauthorized user access. Users shall be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment;

d) The University shall enforce protection mechanisms for unattended user equipment. Users shall ensure that unattended equipment has appropriate protection. Equipment installed in users areas, e.g. workstations or file servers - may require specific protection from unauthorized 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) The University shall enforce network access control policy to protect networked services to both internal and external services. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring: appropriate interfaces between the organization's network and networks owned by other organizations, or public networks; appropriate authentication mechanisms for users and equipment; appropriate mechanisms for remote user diagnostic; and control of user access to information services;

f) The University shall enforce the usage of operating/software system access controls. Also, logical access to software systems and application shall be restricted to authorized users. In addition, to prevent unauthorized computer access, security facilities at the operating system level – there shall be restricting access to computer resources. The audit logs shall include information for: identified and verified identity, and if necessary the terminal or location of each authorized user; recorded successful and failed system accesses; provided appropriate means for authentication; and restricted connection times of users; and

g) The University shall 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 specific ways of working cause. When using mobile computing the risks of working in an unprotected environment shall be considered and appropriate protection measures applied. In the case of tele-working UDSM shall apply protection to the tele-working site and ensure that suitable arrangements are in place.

6.7 Systems Acquisition, Development and Maintenance

6.7.1 Issues

The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements need to be identified and agreed prior to information systems acquisition and development.

6.7.2 Objectives

The University needs to ensure that security services became part of the offered ICT services, implying that security must be built into information systems that UDSM owns. ICT services include infrastructure, business applications and user-developed application.

6.7.3 Policy Statements

a) The University shall develop, implement and monitor business security requirements for ICT services to be acquired and developed. The requirements shall include needs for fall back arrangements, and business requirements for new systems. 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 included during or after implementation;

b) The University shall establish security requirements and appropriate controls that reflect the business value of all business information assets, applications and ICT resources involved, and the potential business damage, which might result from a failure or absence of security;

c) The University shall establish mechanism to prevent loss, modification, or misuse of user data in application systems. Mechanism shall include implementing appropriate controls and audit trails or activity logs designed into application systems;

d) The University shall enforce usage of Cryptographic controls. The technique shall be used 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 IT/ICT projects and support activities are conducted in a secure manner. Maintaining system integrity shall be the responsibility of the user function or development group to whom the application system or software belongs.

f) The University shall enforce Security in development and support processes so as to maintain security of software & systems, applications, business information, projects, and support environments. Managers responsible for application systems shall also be responsible for the security of the project or support environment. They shall ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

g) The University shall enforce control mechanism to monitor security vulnerabilities and threats for outsourced software development. Additionally, where 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 audit of the quality and accuracy of work done; contractual requirements for quality of code; and testing before installation to detect Trojan code, backdoors, and such other security problems.

6.8 Security Incidents and Response Management

6.8.1 Issues

Incident management responsibilities and procedures are very important in ensuring a quick, effective and orderly response to security incidents.

6.8.2 Objectives

The University needs to be able to adequately respond to, manage, and timely recover from security incidents.

6.8.3 Policy Statements

a) The University shall form a Computer Security Incident/ emergency Response Team (CSIRT/CERT) composed of staff members with expertise from the UDSM's IT/ICT technical units, legal unit, and academic units. The team shall be responsible for responding to suspected ICT security incidents by identifying and controlling the incidents and reporting all findings to the technical team for proper measures and later to UDSM management (steering committee) for noting;

b) The University shall enforce mechanisms for ensuring all events (event logging) that could pose potential loss of data, breaches of confidentiality, unauthorized access or change to systems are identified. Audit logs recording exceptions and other security-relevant events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. Any events shall be reported immediately to the IT/ICT service desk either by email, telephone or any other means; and

c) The University shall enforce control procedures to recover from all potential types of security incidents, including: information system failures and loss of service, denial of service, errors resulting from incomplete or inaccurate business data; and breaches of confidentiality. In addition, to normal contingency plans (designed to recover systems or services as quickly as possible) the procedures shall also cover: analysis and identification of the cause of the incident, planning and implementation of remedies to prevent recurrence, if necessary, collection of audit trails and similar evidence, communication with those affected by or involved with recovery from the incident, and reporting the action to the appropriate authority.

6.9 Risk Assessment and Treatment Management

6.9.1 Issues

The University is facing a number of security issues including cyber-attacks, viruses and malicious code. Consequently, implementing appropriate security risk assessment and mitigation measures is necessary.

6.9.2 Objectives

The University is running a number of critical business information assets and ICT resources in its network infrastructure. It is imperative that UDSM put in-place appropriate security measures that would ensure a security risk-free network infrastructure.

6.9.3 Policy Statements

a) The University shall establish comprehensive and up-to-date ICT security risk assessment standard procedures for identifying security vulnerabilities and threats posed to critical business information assets and ICT resources;
b) The University shall enforce comprehensive and up-to-date ICT security standard for risk mitigation that would enhance confidentiality, integrity and availability of critical business information assets and ICT resources; and
c) The University shall form a Security Risk Assessment and Mitigation Team (SRAMT) - 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 for the same. Team functions and composition is to be established by CERT.

6.10 Business Continuity Management

6.10.1 Issues

The University ICT environment is under an increased exposure to increased security issues that may affects the smooth operations of its core business processes which rely on ICT. The issues may include cyber-attacks, viruses and malicious code; system unavailability due to hardware and software failures, aged ICT equipment, frequent power failures, fire, theft, and damages due to the acts of nature. Consequently, creating and implementing an effective and efficient Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP) that address these security problems and help in recovering from the likely disruptions thereof is critically important.

6.10.2 Objectives

Business continuity management is principle aimed at ensuring the University critical business information and ICT assets are free from any security risk and disruptions either physically or logically. It is critically important that the University identify and classify all critical business information assets and ICT resources including physical and electronic assets, such as ICT facilities, hardware, software and other facilities and power supply (electricity); and ensure that state-of-the-art Business continuity and disaster recovery planning (BCP/DRP)for these are in place.

6.10.3 Policy Statements

a) The University shall identify resourceful IT personnel to be imparted with BCP and DRP related specialised training periodically;

b) The University shall establish appropriate mechanisms that would ensure trained and authorised personnel have access to, and securely perform BCP and DRP processes regularly as defined in the procedures;

c) The University shall develop suitable BCP for the classified critical business information asserts and ICT resources. Subsequently, establish plans and processes for security risk and impact analysis and assessment of the loss of critical business information assets and ICT resources in the event of disaster.

d) The University shall establish suitable DRP for the identified and classified critical business information and ICT assets. In addition The University shall develop procedures for periodically review and update listing of the identified and classified critical business information asserts and ICT resources; and

e) The University shall enforce control mechanisms that would ensure, on periodic basis, BCP and DRP systems are periodically tested and reviewed to ensure its effectiveness.

6.11 Security Compliance, Monitoring, Disciplinary and Review Management

6.11.1 Issues

The University has different players when it comes to implementation and use of critical business information assets and ICT resources; these include but not limited to: users, IT staff and third parties (service providers). Consequently, greater possibility of violating the policy; thus, to minimize violation of the same - it is critical for the University to have in place proper proactive and reactive mechanisms for monitoring and accommodating the anticipated changes of ICT environment and the associated technologies in a timely manner. These shall include security postures such as ethical, regulation, legal and technical procedures and standards that govern secure implementation and use of critical business information assets and ICT resources.

6.11.2 Objectives

The University ICT industry, UDSM environment and users are very dynamic. This entails UDSM to have proper mechanisms for ensuring proper compliance and monitoring, disciplinary and timely review of this policy.

6.11.3 Policy Statements

a) The University shall develop and implement rules and procedures that would assist in ensuring compliance while implementing the policy. Any violation of the policy would attract appropriate penalties as defined in the rules and procedures;

b) The University shall establish and enforce appropriate systems audit mechanisms for monitoring, checking and enforcing compliance requirements. The mechanism shall involve the use of automated tools that provides real time notification of detected wrongdoing and vulnerability exploitation; such tools include intrusion detection system logs, Firewall logs, User account logs, Network scanning logs, Application logs, Data backup recovery logs, Help desk logs, and error log files;

c) The University shall develop compliance mechanisms for enforcing adherence to ICT security policy and standards, aimed at ensuring that no individual attempts to gain unauthorized access to any ICT resources or in any way to wilfully damage, alter, or disrupt the operation of ICT resources. Failures to comply with, the University policies and regulations, and national laws, disciplinary measures shall be taken against those responsible;

d) The University shall establish and enforce the usage of appropriate mechanisms for conducting periodic review of users, third-party agreements and contracts (SLAs /OLAs) to see that they comply with the University policies and national laws. In-case of any violation, the findings shall be reported to appropriate authorities;

e) The University shall establish and enforce usage of standard procedures to handle any exceptional case that requires exemption from the security treatments defined in this policy, in an event that there will be a need for not complying to any part of the policy; and

f) The University shall establish an ICT Security Policy Implementation and Review Team (SPIRT) to review and update this policy to match with the dynamicity of ICT requirements at least once a year. The review shall cover assessment of security establishing the existing ICT resources, the associated security risk assessment profile, security mitigation postures, SLA/OLA etc.

7. ICT Security Policy Implementation Documents

The implementation this policy shall require development and enforcement of a variety of short documents which shall be referred to **as policies, rules, regulations, procedures, or standards** as circumstances so requires. These in their totality are the supporting documents for the Implementation of this ICT Security Policy structure once approved:

8. ICT Security Policy Implementation Teams

In addition, to the documents described in chapter 7 above the implementation of the policy would require formation of ICT security teams as follows:

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

9. Document Management and Control Data

In order to ensure proper management and ownership of this document shall be owned by the Vice Chancellor and approved by the Council. The following information will be recorded:

Prepared by: *UDSM*

Owned by: *Vice Chancellor*

Approved by: *UDSM Council*

Date approved:

Review date:

Past review dates: *N/A—first version*

Amendment dates:

Bibliography

ISO-27K, ISO 27005 (2008). Code of practice for Information Security Risk Management. [Retrieved from: http://www.iso27001security.com/html/ iso27000.html, last accessed April, 2014].

ITIL (2007). *Introduction to the ITIL Service lifecycle*. [Retrieved from: http://www.best-management-practice.com/Publications-Library/IT-Service-Management-ITIL/ITIL-Version-3/The-Introduction-to-the-ITIL-Service-Lifecycle/, last accessed April, 2014]

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.

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.

Tz-eGov (2008). Tanzania e-Government Strategy. [Retrieved from: http://www.tanzania.go.tz/, last accessed March, 2014]

Tz-ICT (2003). Tanzania National ICT Policy. [Retrieved from: http://www.tanzania.go.tz/, last accessed April, 2014]

Tz-TCRA (2010). Tanzania Communication Regulatory Authority. [Retrieved from: http://www.tcra.go.tz, last access February, 2014].

UDSM-ICTM, (2007). The University of Dar es Salaam, ICT Master Plan (2008 – 2012), September 2007

UDSM-ICTP, (2006). The University of Dar es Salaam, ICT Policy, May 2006

UDSM-ICTSP, (2014) Initial draft of UDSM ICT Security Policy and Regulations, February, 2014.

UDSM, (2012)Risk Register of University of Dar es Salaam (DSM)

UKL, (2008). The Kindston University London – ICT Security & Usage Policy. *[Retrieved from: http://national3.com/i/ict-security-usage-policy---kingston-university-london-%E2%80%93-study-e3865-pdf.pdf, last access April, 2014]*.

UO, (2012). The University of Oxford – Information Security Policy. *[Retrieved from: http://www.it.ox.ac.uk/media/global/wwwitservicesoxacuk/sectionimages/security/Information_Security_Policy_2012_07.pdf, last access April, 2014]*.

USQ, (2014). The University of Southern Queensland – ICT Information Management and Security Policy. *[Retrieved from: http://policy.usq.edu.au/ data/render/13340PL_files/13340PL.pdf, last access April, 2014]*.

Appendix – Additional Definitions

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

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

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.

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

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.

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.

Security Incident - any action or activity that compromises the confidentiality, integrity, or availability of ICT resources

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 UCC 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

Information Asset – refers to any data or information, as well as related equipment that contains or processes data or information that is relevant to UCC functions.

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.

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 fulfill 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