UNIVERSITY OF DAR ES SALAAM
DAR ES SALAAM UNIVERSITY COLLEGE OF EDUCATION (DUCE)

ICT SECURITY GUIDELINES

JUNE, 2020

Table of Contents

GROSSARY AND ABREVIATIONS

Glossary

Users - refers to all College Stakeholders including College employees and students, and third party (contractors, visitors, interns, filed students) who make use of any ICT resources at the College.

System Administrator (SA) - refers to any ICT staff regardless of their job descriptions titles.

Designated System Administrator (DSA) - refers to ICT staff who has been commissioned to administer various computer systems at the College.

Abbreviations

BCP	–	Business Continuity Plan
BIOS	–	Business Continuity Plan
CCTV	–	Closed Circuit Television System
CD	–	Compact Disk
CD-ROM	–	Compact Disk –Read Only Memory
DHCP	–	Dynamic Host Configuration Protocol
DMZ	–	Demilitarized Zone
DNS	–	Domain Name System/Domain Name Service
DoS	–	Denial-of-Service
DRS	–	Disaster Recovery Site
DSA	–	Designated System Administrator
FMIS	–	Financial Management Information System
HR	–	Human Resources
HRM	–	Human Resources Management
ICT	–	Information and Communication Technology
IDS	–	Intrusion Detection Systems
ID	–	Identification
IP/X	–	Internet Protocol/Exchange
IPS	–	Intrusion Prevention Systems
ISP	–	Internet Service Provider
LGAs	–	Local Government Authorities
MAC	–	Media Access Control
MDAs	–	Ministries, Independent Departments and Agencies

NIDS	–	Network Intrusion Detection Systems
NIPS	–	Network Intrusion Protection Systems
PC	–	Personal Computer
PCRF	–	Password Change Management Request Form
SA	–	System Administrator
USB	–	Universal Serial Bus
UPS	–	Uninterrupted Power Supply

1 OVERVIEW

1.1 Introduction

Information and Communication Technology (ICT) plays an increasingly important role in facilitating the realization of College's mission and vision. It is critical to ensure Confidentiality, Integrity and Availability (CIA) of the information assets so as to support College's core business functions. The College recognizes that ICT security is an issue for the whole College 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 and performance of the College. The College decided to introduce and have in place ICT Security Policy (2019).

In order to manage the risks associated with ICT, the College ICT Security Policy (2019) requires that the College formulates guidelines that will address the following focus areas: Assets Management Security; Communication and Operational Management Security; Access Control Management and Systems Acquisition, Development and Maintenance.

Therefore, this Information, Communication and Technology (ICT) Security Guidelines outlines appropriate use of the College's Information, Communication and Technology resources. It outlines acceptable guidelines for users of ICT resources that include employees, students and other stakeholders. The ICT resources include; computers, printers, programs, data, Local Area Network, emails, CCTV, intranet and the internet.

1.2 Objectives

The ICT security guidelines intends to enable users to properly use and secure the College ICT resources by understanding the acceptable and unacceptable behaviors, conducts and practices in the use of the resources and sanctions for failure to comply with the acceptable behaviors.

The Specific Objectives of the Guideline:

i. To ensure that ICT resources and services are used in an appropriate and responsible manner;
ii. To ensure that only authorised users have access to the ICT resources by implementing the use of password controls; door access cards etc;
iii. To safeguard the integrity and security of ICT resources; and
iv. To ensure consistent understanding of users responsibilities and limitations when using ICT resources and services.

1.3 Scope

These Guidelines apply to all users of the College ICT resources including employees, students, and authorised users.

1.4 Disclaimer

This document provides guidance on the proper use of ICT facilities at the College, however, it is not by any way exhaustive. All users are obliged to comply with this guideline, College ICT Policy (2019), ICT Security Policy (2019) and Government ICT related Policies and Guidelines.

2 ICT SECURITY GUIDELINES

The College considers ICT security as crucial undertaking to safeguard its ICT resources by mitigating the associated risks and enabling users to perform their daily duties effectively and efficiently. As such, students, employees and other stakeholders are required to make good use of ICT resources while observing ethics and security guidelines to the fullest extent in pursuit of College's goals and objectives.

2.1 Unacceptable Behaviour

2.1.1 Creation, display, production, down-loading or circulation of offensive material in any form or medium.

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

2.1.3 Deliberately introducing viruses, worms, trojan horses or other harmful or nuisance programs or file into any College ICT facility, or taking deliberate action to circumvent any precautions taken or prescribed by the College.

2.1.4 Loading into the College ICT resources any device or software without permission from the Deputy Principal (Administration).

2.1.5 College's Information Systems shall not be installed on any personal ICT facility without permission from the Deputy Principal (Administration).

2.1.6 Removing or interfering with output of the ICT resources belonging to another user.

2.1.7 Failure to note and report on any observed or suspected security incidents, security weaknesses or threats.

2.1.8 Allow unauthorised person to use resources assigned to him/her without prior authorization.

2.1.9 It is further unacceptable for any person to use College's 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 commercial purpose;
iv. to send threatening or harassing messages, whether sexual or otherwise;
v. to access or share sexually explicit, obscene, or otherwise inappropriate materials;
vi. to infringe any intellectual property rights;
vii. to gain, or attempt to gain, unauthorized access to any computer or network;
viii. for any use that causes 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 or impersonate either the College or a person's role at the College ;
xi. to distribute chain letters; spam emails;
xii. to access online gambling sites; and
xiii. to libel or otherwise defame any person.

2.2 Use of ICT Assets

2.2.1 Users shall not disclose, or disseminate to unauthorized person, any information or data that they came across during system access unless it is for public consumption.

2.2.2 Users shall not access or try to access information than what was granted to access.

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

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

2.2.5 Users shall not use any College ICT resources for any personal activities that are prohibited under the law.

2.2.6 Messages, postings and blogs shall not disclose any proprietary or confidential information about College or College's clients, including client contract information, internal policies, standards, procedures, processes, guidelines or financial information.

2.2.7 Any comments or postings made regarding user's colleagues or other individuals shall not breach their rights, including the right to data privacy and any comments or postings shall not adversely affect the College reputation.

2.2.8 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.

2.2.9 The College shall not provide backup arrangements for personal applications and downloads, but may provide any support to help manage employee personal files.

2.2.10 Any downloaded software, music or other data, which is for personal use, that is found to or is suspected of interfering with the performance of the College's computer/network or is inappropriately licensed shall be removed from the computer by SA.

2.2.11 All users of workstations, PCs and laptops should ensure that their screens are clear of data when not in use. Moreover, computers should be set so that they automatically switch to a standby mode after a period of inactivity. A password should be needed to regain access to the screen.

2.2.12 Users should ensure that they log off and shut down, if they expect to be away from their desk or work area for a prolonged period and at the end of the working day before they leave office premises.

2.2.13 All software development, acquisitions, deployment and usage at the College should be coordinated centrally by ICT Department to ensure conformity to predefined standards.

2.2.14 Users, before acquiring any software to be used by the College, should seek audience with the ICT department for proper guidance.

2.2.15 On acquiring software, proper procurement procedures should be followed as stated in the Public Procurement Act and its Regulations.

2.2.16 All software acquired by DUCE should have documentation manuals and bear legitimate licenses.

2.3 Email Security

2.3.1 College's employees should have official DUCE email address that will be provided by the ICT Department.

2.3.2 College's employees email accounts that will be created after coming into force of these guidelines will have a format of firtsname.lastname@duce.ac.tz

2.8.1 Emails addressed to other Institutions or to individuals outside the College must clearly identify the sender by full name, position and contact address at the College.

2.8.2 NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying the computer recycle bin.

2.8.3 If users suspect or discover e-mail containing computer viruses or phishing attacks, they should report the incident to the SA.

2.3.3 Users should use e-mail responsibly and preferably for official matters.

2.3.4 Users should not open or forward any e-mail from unknown or suspicious sources.

2.3.5 Users should not copy or forward chain e-mails. Chain emails can disrupt email services and other internet services on College network.

2.3.6 The e-mail system should not be used to commit unlawful and illicit acts.

2.3.7 Users should avoid publishing e-mail address to unknown individuals or expose users' credentials by filling forms from dubious links and websites.

2.3.8 Users should use separate e-mail addresses different from their office e-mail addresses when participating in public newsgroup or chat rooms, to avoid their office e-mail addresses and/or mail systems to become a target of spam.

2.3.9 Users should not reply to spam because most return addresses are not legitimate and would only result in the generation of non-delivery messages thus increasing the amount of undesired traffic.

2.3.10 Users should control spam by using e-mail filtering tools in e-mail software that allow users to block or screen out spam by defining some simple filtering rules.

2.3.11 User should not send e-mails using another person's e-mail account.

2.3.12 Only encryption authorized by the College should be used to encrypt e-mails.

2.3.13 The College reserve the right to inspect, monitor and disclose the contents of any email created, sent, received or forwarded by using the College computer network or email system.

2.3.14 Users must not spoof or otherwise falsify a sender address.

2.3.15 Users are not authorised to try and gain access to another employee's data files and email without the consent of the latter.

2.3.16 Users are not permitted to 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, sexual orientation, age, disability, religious or political beliefs.

2.3.17 If an employee vacates the College for any reasons provided he or she is no longer the College beneficiary employee, the office of the HRM should officially communicate this information to ICT department and thereafter the employee's DUCE email account will be deleted from the DUCE Email database within two months and his or her data will not be recovered.

2.3.18 Users should not share email accounts passwords. For officers using management emails must handle the email account to another officer and report to the ICT department for the issuing of a new password by filling a Password Change Request Form (PCRF)

2.4 Internet and Intranet Usage

2.4.1 Internet access shall be provided to users to support daily activities upon being issued with access credentials.

2.4.2 College stakeholders excluding employees and students will be required to fill Internet Request Form (IRF) for internet services.

2.4.3 Academic Staff should adhere to the University of Dar es Salaam Examination Guidelines.

2.4.4 Unless specifically authorized, on item by item basis, users are strictly prohibited to use the Internet for:

i. Downloading of games or shareware programs.
ii. Ordering (shopping) of personal items or services.
iii. Playing of any games or participating in any on-line contest or promotion.
iv. Deliberately propagating computer viruses, worms, Trojan horses or trap door.
v. Disabling or overloading any computer system or network or to attempt to disable, defeat or circumvent any system intended to protect the privacy or security of another user.
vi. Downloading or distributing pirated software or data.

2.4.5 The use of the Intranet is intended exclusively for the work undertaken for or by the College.

2.4.6 Users should act responsibly and maintain the integrity of the data/information within the Intranet/Internet all the times.

2.4.7 All information/data posted to the Intranet/Internet should be checked for malicious software.

2.4.8 Internet usage activities of users may be monitored by the ICT team.

2.4.9 Users are expected to protect their personal user credentials, such as user IDs and passwords. These should in no case be given to anyone (including colleagues). These credentials shall not be stored on Internet browsers.

2.4.10 Users shall not access College confidential data via a public computer such as in a cybercafé.

2.4.11 It is strictly prohibited to download unapproved software using the College Internet access and install same on College devices.

2.4.12 Users shall not use College Internet access to download movies, pictures and music files unless work related.

2.4.13 All downloaded files from the Internet should be scanned using dependable anti-virus detecting software before they are opened on College devices.

2.4.14 Users must not deliberately try to bypass security controls on the College systems to access the Internet.

2.4.15 Users are not allowed to disable the anti-virus protection running on their computers for browsing the Internet.

2.4.16 Users shall not use the Internet resources provided to them at work for sexual or racial harassment.

2.4.17 Users must not use the College Internet to gain unauthorised access to other systems or web sites.

2.4.18 Users of portable devices accessing the Internet from public places should make sure that proper security measures are maintained, such as not connecting to unsecured network.

2.4.19 Users are expressly forbidden from making unauthorized alterations or extensions to the network.

2.4.20 A register of network devices, their access restrictions and the protocols in use should be kept by the DSA.

2.4.21 All changes to network configurations should be recorded in the confidential register, along with authorization for the changes.

2.4.22 Users should be permitted to use only those network addresses issued to them by the DSA.

2.4.23 Virtual networks should be set up for specific groups of users. These groups should have Group User Access Profiles, on which the user access profiles of individual team members should be based.

2.4.24 Remote College users should connect to servers using a secure communication channel such as Virtual Private Network on dedicated communications lines with end-to-end encryption.

2.4.25 Results/Logs from the firewall should be reviewed by DSA to confirm there have been no unexpected attempts to connect.

2.4.26 Users should not extend or re-transmit network services and traffic in any way i.e. they should not install a router, switch, hub, or wireless access point to the systems network without being approved.

2.4.27 Users with administrative privilege should not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, system users should not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the system network infrastructure.

2.5 Use of Passwords and Authentication

2.5.1 Granting of access rights to some College ICT resources will be by the provision of secret authentication methods, commonly the username(s) and password(s), thus the College ICT facility users;

i. Must not use another user's username or password, nor allow any password issued to them to become known to any other person.
ii. Must not leave ICT resources unattended after logging in.
iii. Must notify the designated authority of any change in their status which may affect their right to use ICT resources.
iv. Must ensure passwords used not based on personal information like family names, year of birth or login name.
v. Password must be alphanumeric, i.e. include numbers, upper and lower case letters and special characters.

2.5.2 Passwords must neither be stored as a clear text nor written onto hard-copy surfaces, such as scratch papers, notepad, etc. Also, storing password in a computer file, whether on your hard drive or on flash disk, can make it accessible to unauthorised users.

2.5.3 Initial passwords that have been assigned as original user-ID passwords must be changed at the first user log-on, whether the information system forces them or not. Passwords should be chosen by the user not by the systems administrator.

2.5.4 Password protected screen-savers on all PCs and servers must be implemented. The screen-savers must be automatically activated after at most five (5) minutes.

2.5.5 For systems that cannot have screen saver functionality, users must log off from their connection session when they plan to be away from their terminal or when they have completed their tasks.

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

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

2.5.8 Users are required to change their systems passwords at most ninety (90) days, in case of any suspected breach of confidentiality, the password must be changed immediately.

2.5.9 All User ID and default passwords supplied by third parties must be changed following the installation of the software.

2.5.10 A Password Management Request Form (PMRF) should be filled by users acquiring new passwords for various accesses at the College.

2.6 Security of ICT Equipment

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

2.6.2 Any equipment or media taken off the premises of the College shall not be left unattended in public place. While travelling, users of portable devices are responsible for ensuring that proper physical handling is maintained. It is advisable to keep visual control over these devices at all times. For example, laptops should be carried as hand luggage and disguised where possible when travelling or laptops should not be left in back seats of cars as they can easily be stolen.

2.6.3 When ICT equipment is missing or stolen should immediately be reported to the SA and Police, and then other internal reporting processes will continue.

2.6.4 Users must take every precaution to avoid damage to equipment caused by eating or drinking in its vicinity.

2.6.5 The equipment must be switched off properly before leaving the office.

2.6.6 Users are not allowed to alter any software or hardware installation.

2.6.7 Users of the College equipment in public areas shall take proper safeguards to ensure that unauthorised viewing of confidential or secret data is avoided, such as ensuring that their device is not left unattended, screens are locked when not in use and confidential information is not displayed on screens in public areas.

2.6.8 Off-premises laptops containing confidential information shall be protected with an appropriate form of access protection, e.g. passwords, smart cards, or encryption, so as to prevent unauthorised access.

2.6.9 Users shall observe manufacturers' instructions for protecting equipment at all times, for example, necessary precautions should be taken to protect equipment against exposure to strong electromagnetic fields.

2.6.10 In the event that the user faces an operational or security incident he should immediately report it to the SA.

2.6.11 Rooms that host servers should be non-smoking zones, fireproof, fitted with smoke detectors and have automatic or portable fire extinguisher systems.

2.6.12 Smoke detectors and fire extinguishers should be regularly tested to ensure that they are in good order and all tests have to be documented.

2.6.13 Materials which can easily catch fire should be disposed-off and those documents which are still in use should be stored in a secure place.

2.6.14 Activities such as rewiring, welding or cutting, undertaken as part of structural changes to the premises of ICT resource, should be monitored by ICT staff, so long as there is proof of safety of new wiring required.

2.6.15 Clear fire instructions should be available and in the event of fire, these instructions should be followed.

2.6.16 Servers should be well mounted on racks and other equipment should be kept off the ground, placed on tables or desks.

2.6.17 The College offices should be adequately air conditioned to provide conducive environment for the ICT equipment.

2.6.18 UPS should be installed as appropriate to all ICT resources.

2.6.19 Non-critical electrical equipment, especially high power consumption equipment such as photocopiers, printers and kettles should not be connected to UPS sockets.

2.6.20 Movement of ICT equipment owned by the College should be authorized by the relevant authority in written form. Proper record should be kept for such movements.

2.6.21 All students, employees and other stakeholders must declare personal ICT equipment at the College entrance.

2.7 Mobile Devices Usage

2.7.1 Mobile devices connected to the network should adhere to the following guidelines:

i. Their operating system and any installed software shall be fully patched and kept up to date.

ii. Up-to-date antivirus and antispyware protection shall be installed 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 College network.

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

iv. The mobile device shall not have a blank password and all default passwords shall be changed.

2.7.2 Users must take appropriate measures to protect the mobile devices against accidental loss, damage or theft.

2.7.3 College network and system passwords must not be stored on mobile devices unless it is a system limitation.

2.8 Anti-Virus Process

2.8.4 Any suspected computer threats or viruses should immediately be reported to the SA.

2.8.5 Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

2.8.6 Always scan a removable media such as flash disks, external HD from an unknown source for viruses before using it.

2.8.7 Back-up critical data and system configurations on a regular basis and store the data in a safe place.

2.8.8 When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

2.8.9 New viruses are discovered almost every day. Periodically check the validity of antivirus software.

2.9 Closed Circuit Television (CCTV) Usage

2.9.1 Materials or knowledge secured as a result of the use of CCTV systems shall not be used for any personal or commercial purposes unless authorised by the Deputy Principal Administration.

2.9.2 Any CCTV recorded data shall only be released for use in any investigation and with the written authority from the Deputy Principal (Administration).

2.9.3 Daily monitoring and management of CCTV system shall be the responsibility of the Auxiliary Police or any other officer assigned to do so by the Deputy Principal (Administration).

2.9.4 Access to the CCTV system and stored images shall be restricted to authorised personnel only.

2.9.5 Users shall be granted access to the Control Room on a case-by-case basis and only then on written authorisation from Deputy Principal (Administration).

2.9.6 All staff working in the CCTV control room shall be made aware of the sensitivity of handling CCTV images and recordings.

2.9.7 Any complaints about College CCTV system should be addressed to the Office of the Deputy Principal (Administration).

2.10 Access Controls

2.10.1 Access control badges/cards will be issued by the Deputy Principal (Administration) and remain the property of the College. Biometric gargets where applicable may be installed for access control.

2.10.2 Users will obtain and display their access control badges/cards, while on the office and where all access is controlled.

2.10.3 Users are forbidden to use access control badges/cards assigned to another person.

2.10.4 The protection of the access control badge/card is vital responsibilities for each cardholder.

2.10.5 Any loss of staff access card should be immediately reported to SA for immediate discontinuation of the service.

2.10.6 All the access control transactions records shall be maintained by Deputy Principal (Administration).

2.11 Software Use and Licensing

2.11.1 Only suitably licensed software may be used to perform the business of the College.

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

2.11.3 College retains the rights to applications and source codes developed on College's ICT resources. This includes ICT applications developed and facilitated by the College.

2.11.4 Users shall not install College's licensed applications and software for use on non-College ICT resources.

2.11.5 If personal use software or media files are found to interfere with the normal operation of College's systems or are considered to pose an unacceptable risk to the College then they must be removed.

2.11.6 ICT department will maintain a database of properly licensed software plus records of software licenses and proof of ownership in relation to Intellectual Property Rights maintained for business purposes.

2.11.7 ICT department will perform periodic scans of all PCs and mobile devices to identify installed software. Instances of software identified via periodic scanning of personal computers will be reconciled with licensing data and anomalies addressed in a timely manner. Unlicensed software will be removed. Responsibility for such anomalies will be assumed to rest with the person to whom the PC is assigned.

2.11.8 Software applications that are no longer needed should be uninstalled.

2.11.9 Software should be used for intended purpose as stipulated in terms and conditions of the software.

2.11.10 Before a user is permitted to use particular software, the designated department should instruct users on the proper usage of the particular program.

2.11.11 Designated department should inform users on terms and conditions included in the license agreement accompanied by the program.

2.12 Technology Equipment Disposal

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmental and a legal requirement. In addition, hard drives, USB drives, CD-ROMs and other storage media store College data, some of which are considered sensitive. In order to protect the data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

The following guidelines shall apply for the disposal of any technological equipment:

2.12.1 ICT equipment such as computers, servers that have reached the end of their useful life, the ICT department will securely erase all storage medium in accordance with current industry best practices before disposal.

2.12.2 Equipment which is working, but reached the end of its useful life to the College will be made available for purchase.

2.12.3 No warranty or support will be provided with any equipment sold.

2.12.4 Any equipment not in working order or remaining from the procurement process will be disposed of according to applicable environmental guidelines.

2.12.5 All disposed equipment must be removed from the College Asset Register.

2.12.6 Failure to properly dispose of technology equipment can have several negative ramifications to the College including fines and negative customer perception.

2.13 Employee Workplace Practices and User Account Termination

Users account termination may arise due to employment suspension, termination, leave, retirement, death, transfer or job change.

The following are measures to be taken by HRM and ICT departments during termination process:

i. Manager HRM should provide updated information of existing employees to the ICT Manager on regular basis.
ii. Manager ICT should act upon the updated information of employees from Manager HRM. The Manager ICT should enquire updated employees' information from Manager HRM if the information is not received on time.
iii. Where applicable, head of department should provide information for employees who are on leave, so that their system account where necessary be deactivated and reactivated when they report back to office.
iv. Manager ICT should ensure that the system account for employee who is leaving the organization is terminated.
v. All ICT assets for any terminated staff should be returned to respective department or unit.

2.14 Management of Third Parties

All external organizations or individuals who wish to supply services to the College will be bound to follow these ICT security guidelines as part of their contractual terms. Management of third parties includes issues on third party verification, service level agreements, outsourcing, cloud computing services, equipment leasing, maintenance and support services and issues pertaining to Internet Service Providers (ISP's).

In a scenario where vendors fail to deliver service as per contracts appropriate legal action will be taken against them according to terms and conditions as stipulated in the contract.

3 IMPLEMENTATION, REVIEWS AND ENFORCEMENT

3.1 Implementation and Reviews

3.3.1 This document shall come into operation once approved by the College Governing Body

3.3.2 Failure to observe this guideline may subject individuals to loss of ICT resources access privileges, disciplinary action or both.

3.3.3 This document may be reviewed from time to time on accounts of changes on business environment of the College.

3.3.4 Any amendments to this guideline shall be approved by the Governing Board.

3.2 Roles and Responsibilities

It is the responsibility of any person using College's ICT resources to read, understand, and follow these guidelines. In addition, users are expected to exercise reasonable judgement in interpreting these guidelines and in making decisions about the use of ICT resources. Any person with questions regarding the application or meaning of statements in this policy should seek clarification from the Deputy Principal (Administration).

The Manager responsible for ICT shall enforce compliance with these guidelines by access revocation and removal to College systems and networks and where applicable to trigger the disciplinary process.

3.3 Monitoring and Evaluation

Computer Security Incident/ Emergency Response Team (CSIRT/CERT) shall be responsible to monitor and evaluate the implementation, enforcement and compliance of these guidelines and recommend to the College Management appropriate measures for improvement.

REFERENCES

1. DUCE ICT Policy (2019)
2. DUCE ICT Security Policy (2019)
3. DUCE Business Continuity and Disaster Recovery Plan (2018)
4. Acceptable ICT Policy Use available at https://www.ega.go.tz/standards accessed on 13th March 2020.
5. Ministry of Finance, United Republic of Tanzania (2012; ICT Security Guidelines) available at https://www.mof.go.tz/docs/ICT%20SECURITY%20GUIDELINES.pdf, accessed on 13th March 2020.