SOKOINE UNIVERSITY OF AGRICULTURE

PROPOSED INFORMATION COMMUNICATION TECHNOLOGY

REGULATIONS

As Approved by SUA Council in its 139th Meeting held on 1st October 2015

FOREWORD

Sokoine university of Agriculture (SUA) recognizes that the presence of a capable, effective, and forward-looking Service that will be able to implement the SUA's development policies and deliver services in an efficient and timely manner, is a pre-requisite for fulfilling goals as articulated in the SUA's Mission and Vision. Information and Communication Technology (ICT) development and its wide utilization across the world have made ICT to be used as strategic tool to achieve development goals globally. Increasing capacity of ICT has further been empowered by the growth of a global network of computer networks i.e. the Internet.

By recognizing the impact of ICT in achieving SUA's objectives, the University has deployed several ICT systems for effective and efficient service delivery. Some of these systems can only be accessed internally while others outside the University. The University further understands that ICT systems are vulnerable to attacks and there are threats which need mechanisms to protect organizational ICT resources against threats and attacks. In addition, improper handling (collection, storage, processing and transmission) of organizational data would infringe rules and regulations governing data confidentiality, integrity and availability. Moreover, the University has an ICT unit to oversee proper utilization of ICT resources in the Institution as well as monitor all ICT activities while ensuring that they are conducted according to the best practices.

Thus, this document provides mechanisms for regulating and guiding both, the handling and use of ICT facilities of the University. The Regulations put forward best practice when using University ICT facilities. These Regulations are in line with the National ICT Policy 2003, SUA ICT Policy 2014, and other relevant Institutional policies that aim at creating a proper handling and use of ICT facilities that would enhance service delivery while protecting organizational resources.

In developing this document, several stakeholders have made it possible. Acknowledgment is extended to all stakeholders who in one way or another contributed to making sure that the SUA ICT regulations are in place.

It should be clear that, in a scenario where an ICT facility user fails to comply with these Regulations; Disciplinary measures will be taken against them as per Public Service Acts, Regulations, Circulars and other Institutional Directives. It is therefore my expectation that all users will adhere to the regulations set here forthwith.

Prof. Gerald C. Monela
Vice Chancellor
September, 2015

PART I

PRELIMINARY PROVISIONS

Citation 1. This regulation may be cited as Sokoine University of Agriculture information communication technology regulations, 2015

Application 2. This regulation shall apply to the users of SUA ICT resources

Interpretation 3. In this Regulation unless the context otherwise requires- "Access" in relation to any computer system, means entry to, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system or network or data storage medium;

"**Bandwidth**" means amount of data a network can transmit in a certain period of time usually expressed in bits per second;

"Computer system" means a device or

combination of devices, including network, input and output devices capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that perform logic, arithmetic data storage and retrieval communication control and other functions;

“Computer data” means any representation of facts, concepts, information or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"**Cloud computing**" means the delivery of ICT services as a service on computing resources such as applications, software, infrastructure as well as platforms over the Internet without necessarily hosting servers by SUA;

"**Data backup regimen**" means a

system of recording identified data onto portable media.

"**Data storage medium**" means any device, article or material from which computer data or information is capable of being stored or reproduced, with or without the aid of any other device or material;

“Device” means electronic equipment which can include:-

a) a computer program, code, software or application;
b) component of computer system such as graphic card, memory card, chip or processor;
c) computer storage component;
d) input and output devices;

"Document" means any recorded information or material, in electronic format or print, which conveys coherent information for human understanding and use.

"**E-resources**" means Information

resources that user accesses electronically including, but not limited to electronic journals, electronic books and other Web-based documents;

"**Free Open Source Software**" means computer software that anyone is freely licensed to use, copy, study, and modify the software in any way, and the source code is openly shared so that people can modify or improve the design and its performance;

"**E-waste**" means non-usable desktop computers, notebook or laptop computers, CD-ROM and DVD equipment, data projectors, digital cameras, telephones, mobile phones and personal digital assistants (PDAs), printers, photocopiers, fax machines and multifunction devices (MFDs), keyboards and similar peripheral ICT devices, servers, hubs, switches, bridges, routers, power supplies and batteries, UPS, scanners, electronic entertainment devices and consoles, and other similar items. This definition includes used electronic equipment destined for reuse, resale, salvage, recycling, or disposal;

“Hyperlink” means a symbol, word, phrase, sentence or image that contains path to another source that points to and causes to display another document when executed;

"**Information and Communication Technologies (ICT)**" means a diverse set of tools, systems, applications and services used for production, processing, storage, transmission, presentation and retrieval of information by electronic means;

"Intellectual property rights" means the rights accrued or related to copyright, patent, trademark and any other related matters;

"**Institutional repository**" means online database for collecting, preserving, and disseminating the intellectual output of an institution. The collection includes but not limited to materials such as journal articles particularly preprints, theses and dissertations, research reports, course notes, and other academic documents;

"**Internet**" means a collection of private and public router-based networks that are interconnected via gateways and exchange points, which all utilize the TCP/IP protocol;

"Internet Protocol Address (or IP Address)" means a unique address that computing devices use to identify itself and communicate with other devices in the Internet Protocol network;

"**Local Area Network (LAN)**" means computer network that spans a relatively small area such as a single building or group of buildings;

"**Management Information Systems**" means information systems used as tools to facilitate the management of corporate functions

"**ICT Equipment**" means any electronic device used for Information and Communication Technologies including desktop computers, laptops, servers, monitors, printers, audio-visual (AV) equipment, software and network equipment;

"ICT facility" means a place or piece of equipment that uses Information and communication technology including physical devices, internet facilities both wireless and wired;

" **ICT unit**" means the University unit dealing with ICT matters in delivering services;

"**Modular object-oriented dynamic learning (Moodle)”** means open source learning platform designed to provide educators, administrators and learners with a single robust, secure and integrated system to create personalized learning environments. This also can refer to Modular Object-

Oriented dynamic learning environment;

"**Parallel Running**" means a process of running a new or amended system simultaneously with the old system to confirm that it is functioning properly before complete migration;

"**Publish**" means distributing, transmitting, disseminating, circulating, delivering, exhibiting, exchanging, printing, copying, selling or offering for sale, letting on hire or offering to let on hire, offering in any other way, or making available in any way;

"**Physical access**" means the ability of a person to gain access to physical facilities (e.g., buildings, computer, server rooms, warehouses);

"Remote site" means a site which is away from the main server which includes but not limited to campuses, colleges, schools and hostels;

"Restricted system" means system

which does not allow unauthorized users to access;

"**Rootkits**" means a type of Trojan that keeps itself, other files, registry keys and network connections hidden from detection;

"**Software Change Management**" means a process of planning, organizing, controlling, executing and monitoring changes that affect the delivery of ICT services;

"**System Administrator**" means person responsible for running and maintaining networked computers, peripherals, and the network itself;

"Spam" means unsolicited messages sent typically to large numbers of users, for the purposes of advertising, phishing, spreading malware;

"**Structured Cabling**" means a set of cabling and connectivity products that integrates voice, data, video, and various management systems of a building (such as safety alarms, security access, energy systems, networks etc.);

“**Transmission Control Protocol/Internet Protocol (TCP/IP**" means a basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network;

"**Trojan**" means a program that appears legitimate but performs some illicit activity when run; It may be used to locate password information or make the system more vulnerable to future entry or simply destroy the user's stored software and data, Trojan is similar to a virus, except that it does not replicate itself;

"**Trusted Cloud Computing Vendor**" means person or company that has high level of confidentiality, uses server, and client authentication, security domains, cryptograph in data separation, and certificate-based authorization;

"**University**" means Sokoine University of Agriculture (SUA);

Uninterruptable power supply (UPS) is an electrical apparatus that provides emergency power to a load when the input power source, typically mains power fails;

"Unsolicited messages" means communication that:

(1) Does not have one of the following qualities

a) the receiver does not consent to such communication and has evidently shown to the sender,

b) at the beginning of the communication, the communication does not disclose the identity of sender and its purpose; and

c) That communication does not give an opt-out option to reject further communication.

(2) The consent requirement is deemed to have been met where-

a) the contact of the addressee and other personal information were collected by the originator of the message in the course of work or business relations;

b) the originator only sends promotional messages relating to its similar products and services to the addressee;

c) the originator offered the addressee the opportunity to opt-out and the addressee declined to opt-out; and

d) an opportunity to opt-out is provided by the originator to the addressee with every subsequent message;

"**User**" means any person authorized to use University ICT facilities;

"**Virus**" means a software used to infect a computer after the virus code is written; it is buried within an existing program and once that program is executed, the virus code is activated and attaches copies of itself to other programs in the computer and other computers in the network;

"**Wide Area Network (WAN)**" means a geographically dispersed telecommunications network, thus computers connected to a *wide-area network* are often connected through public *networks*, such as the telephone system. They can also be connected through leased lines or satellites;

"**Wireless Network**" means network that does not require cable connections.

Disclaimer

4. The University undertakes to provide and operate its ICT resources with reasonable

skill. However, the University accepts no liability for any loss or damage a user may suffer from any failure or malfunction of the University ICT resources or any part thereof.

PART II

GENERAL REGULATIONS

Need of authorization

5. Access to ICT facilities on the systems network shall be restricted unless specifically authorized by registration or any other means by a relevant authority.

Systems Account handling

6. User shall sign "User Access Permission Form" showing that;

   a. password has been received

   b. it will be kept secret

   c. changed frequently or at a moment that a breach of confidentiality is suspected

7. Users shall;
   a. Be responsible for the security of their account passwords including the changing of passwords on a regular basis
   b. Be responsible for all activities that originate from their system accounts, unless proved otherwise.
   c. Make sure that his/her computer is free from viruses, malware and any suspicious window activities, Failure to that will be disconnected from the network if his/her computer becomes infected with viruses, malware or if it displays suspicious network activity.
   d. Agree to abide to all University ICT regulations and guidelines and must comply with the national laws.

8. Only laptop, desktop computers and mobile devices are allowed on the University network. Connection of any wireless access point, cable/broadband router, hub, switch, game console or any such devices to the SUA network must be with permission and assistance of the ICT unit.
9. User shall not publish any material on SUA ICT equipment that may be offensive to the public.

Systems Protection

10. User must keep his/her passwords secure and must not disclose them to, or allow them to be used by any other person.

11. User shall notify the System Administrator immediately if he/she suspects that his /her ICT facilitate account/password has been compromised as guided by the University ICT unit.

12. In case the user does not abide to 10 and 11 shall be responsible for any damage caused

Infrastructure protection

13. User is required to carefully use a University ICT facilities and report faults immediately to the respective authority using verifiable means.

14. User shall not be allowed to extend cabling of the wired network unless special permission is provided by the responsible ICT unit.

System updating and upgrading

15. A user shall
    a. Abide to the terms of copyright laws, software licensing agreements, and contracts that pertain to the University's computing, information, and communications resources.
    b. Keep computers up-to-date with operating system updates and security patches.
    c. Be solely responsible for the actions of any person who accesses their own ICT facilities or system accounts by whatsoever means.

d. Be responsible to stay up-to-date with ICT policy, Regulations and Guidelines.

e. be considerate in the use of shared resources and not perform acts that are wasteful of computing resources or that unfairly monopolize resources (through but not limited to, junk mail, chain letters, games, obtaining unnecessary output, creating unnecessary network traffic, or printing an excessive number of copies of any documents such as resumes, theses, and dissertations).

f. not install, run, or give to another user a program that is intended to or is likely to damage a file or computer system and/or reproduce itself on University computer systems.

g. be restricted to use university owned sensitive data from IT environments in which these data are maintained by university faculty and staff

SUA computer networks

16. User is prohibited

a. To deliberately perform an act that will interfere with the normal operations of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with any component of a local area network (LAN), Intranet, or wide area network (WAN); blocking communication lines and or interfering with the operational readiness of a computer.

b. To attempt to bypass data protection schemes, to uncover a security loophole

c. To mask the identity of a computer account or machine

d. To use Unauthorized and

installation peer to peer file sharing programs

17. User is expressly forbidden unauthorized access to accounts, data or files on SUA ICT resources, or on ICT resources belonging to other person or organizations.

18. Game playing is not allowed on SUA ICT facilities, except as a formal component of a University academic subject or sponsored event or when specifically authorized

19. User is not permitted to use ICT facilities to sell or purchase assignments, or to offer to write assignments or to request help with assignments.

20. Unless authorized by the University, user is not permitted to run business using university ICT facilities.

21. The University reserves the right to withdraw a service or withdraw access for personally owned computers if there is evidence of misuse of ICT facilities

Unauthorized software

22. Software and/or information that infringes the rights of another or that gives unauthorized access to another computer account or system must not be placed on any University-owned computer system or computer connected to the University's network.

Use of Internet

23. Browsing of Internet sites containing pornographic, obscene, and immoral or any other inappropriate content is prohibited as per national laws

24. Unauthorized user must not access or alter restricted portions of the operating system in the computer (e.g. registry) or configuration (e.g. IP Address, Computer Name and Active

Directory settings)

Use of E-mails

Use of office E-mails

25. User must use e-mail responsibly and preferably for official matters.

26. User must not open or forward any email from unknown or suspicious sources.

27. User must not copy or forward chain emails. Chain emails can disrupt email services and other Internet services on networks.

28. If user suspects or discovers an e-mail containing computer viruses or phishing attacks, they must report the incident to the ICT Unit as guided or using verifiable means.

29. The email system must not be used to commit unlawful and illicit acts.

30. User must not reply to spam

Use of personal e-mails

31. User must not send emails using another person's e-mail account.

Computer laboratories Regulations

Labs for university's mission

32. SUA ICT facilities including computer laboratories are for academic, research, outreach and service delivery works only and shall not be used for personal gains.

Proper use of laboratories

33. Unless permitted by the ICT unit responsible, all University Computer Laboratories shall be used for practical sessions purposes only and not for lecturing and/ or theory examinations.

Unacceptable actions in laboratories

34. To protect ICT equipment and other facilities, activities such as Smoking, eating, chewing gums and drinking are NOT allowed in the computer laboratories

ID card requirement

35. Unless permitted by the ICT unit responsible, all persons in the computer laboratories are expected to have their ID cards.

36. Without the ID, the user shall be required to leave the room immediately.

37. Users of the computer laboratories must register their details in the book or any other electronic means provided

38. Mobile phones must be switched off or put in silent mode at all times in computer laboratories.

Prohibited items in computer laboratories

39. The following personal items are forbidden in the computer laboratories unless otherwise permitted by the head of ICT unit:
   a. bags or back packs of any kind
   b. laptops
   c. liquid material
   d. food

40. No any form of storage media shall be inserted into the computer without permission of ICT personnel who will prove that it is free of viruses and other malicious

software.

41. No playing games, watching films, and listening to music are allowed unless they are part of the academic or research work.

42. Any conduct or activity which disturbs the computer laboratory's environment is not allowed.

43. Anyone causing continual disturbance will be asked to leave the computer laboratory. If the offense done is serious enough, the laboratory assistant may call the Security Officers for assistance;
    a. Individuals exhibiting hostile or threatening behavior such as yelling, swearing, or disregarding requests made by laboratories personnel will be asked to leave the laboratories.
    b. Display of personal affection inside the laboratory is

prohibited.

44. The laboratory assistant has the right to advise any user to leave the premises in case the user violates any of the regulation and guidelines.

Offenses and Actions

45. Any attempt to access SUA facilities or another user's computer account or e-mail; or impersonate as another user or create or introduce programs with malicious intent; or involve in software theft; or use SUA facilities to harass any company or individual or send chain or junk mail, shall result into administrative actions including summarily dismissal from service or take legal actions.

46. Any attempt to circumvent network and computer security restrictions imposed by the University (for example running an encrypted tunnel or changing your

computer's MAC address) may be subject to appropriate action by the University organs including legal actions in court.

47. Any violation of these regulations shall lead to disciplinary action and may include the deactivation of the user account.

48. Any breach of these regulations shall be dealt in accordance with National laws, SUA Charter, Staff Regulations, SUA students by laws and any other written laws or guidelines

Objects and Reasons

The main purpose of these Regulations is to provide framework for governance which includes selecting, implementing, and managing Information and Communication Technology (ICT) services by guiding the Institution on how to manage ICT facilities. Moreover, the document intends to protect a diverse set of tools, systems, applications and services used for production, processing, storage, transmission, presentation and retrieval of information by electronic means. ICT encompass a wide range of rapidly evolving and increasingly converging technologies including hardware, software, networks, audio-visual systems, and associated applications.

In addition, the Regulations handling ICT security issues for all users who access SUA's information systems resources. Furthermore, the document provides information for decision makers and other relevant parties on ICT management issues for the purpose of obtaining comprehensive ICT services.

Therefore, this document is meant to translate the SUA ICT policy 2014, National ICT Policy 2003, Tanzania Public Service Act 2002, Public Procurement Act, 2011 and Public Procurement Regulation, 2013 and existing circulars into implementation in the form of guidelines which are easy to follow on the day to day operations.

SUA ICT Vision

SUA utilizing excellent ICT solutions

Mission

To fully integrate ICT in training, research and delivery of services

Bibliography

1. Sokoine University of Agriculture, Information and Communication Technology (ICT) Policy (2014).
2. Sokoine University of Agriculture, Guidelines for Website Contents, (2012).
3. Sokoine University of Agriculture, Staff Regulation, (2013).
4. The United Republic of Tanzania – Ministry of Finance, ICT Security Guidelines, December 2012.
5. Republic of Malawi, Public Service ICT Standards, January 2014.
6. Michigan State University, Faculty and Staff Guide to Computing and Technology, 2010/11
7. The electronic Transactions Act, 2015
8. The cybercrime Act, 2015

Appendices

Appendix 1

Sokoine University of Agriculture
Network Access confidentiality Form

User Details

Access required to Network/System/Application

New User [ ]   Existing User [ ]   Deletion of User [ ]

Full Name_________________________ PF No.___________

Job Title____
Department/School/Campus_________________________

Cell Phone Number __________Email Address__________

Access required to function (s) _____________________

Authority Level where applicable ____________________

I acknowledge that:
My Password will at all times remain confidential to me

I will take all necessary precautions to ensure that no an authorized persons can gain access to my password

Failure to adhere to the above mentioned will be viewed as a serious breach of trust and will result severe disciplinary action

Signature ____

Authorizing Officer

Full Name..
Department..

Work telephone number..
Job Title..

Cell Phone Number _______________________________

Email Address ____________________________________

I confirm that the access required is in the accordance with the user's job description.

Signature: _______________________________________

Appendix 2

SUA ICT Facility Borrowing Application Form

ICT Facilities are available for University staff to borrow for SUA work related purposes. Maximum loan time is one week.

Please note, damage, or loss of the item will result in the corresponding charge being assessed to the individual or department making the booking.

The ICT facility may be borrowed for the following reasons:

• On Campus Meetings SUA Community Events (eg Public Lectures, Open Day) Failure of work computer

The ICT Facility shalll not be borrowed in the following circumstances:

Conference Attendance ( ) Overseas Travel (Personal Home Use ( )

Authorisation must be obtained from your Dean/Faculty or Department. Costs associated with any damage or loss of the laptop will be billed to the Faculty/Department in SUA.

Dates Required: From: ----/-----/-----

To: ----/-----/-----

SECTION ONE *(TO BE COMPLETED BY THE APPLICANT)*

Full Name: ....

Position: ....
Faculty/Dept: ....

Reason for Borrowing: ....

Location Where the ICT facility will be used Mobile
Number...........................Signature:......................
Date: ....

SECTION TWO *(TO BE COMPLETED BY THE AUTHORISING OFFICER)*

Authorization

(To be completed by Dean / Head Head of Department)

The above staff member is authorised to borrow the nominated ICT facility for the period specified. The Centre/Faculty/Department will meet the associated costs if the item is damaged or lost.

Full Name: ....
Position:...
Faculty/Dept:..

Signature: ....   Date: ....

Director ICT Unit Comments

Comments: **...**

Signature: .... Date ....

Appendix 3

Sokoine University of Agriculture

Change Request Form

Change Request #: ______ Department/Faculty: ______

CHANGE REQUEST INITIATION: Originator: ___________________

Phone#: ______________________Date Submitted: ____/____/____

CONFIGURATION ITEM:

Software: ___ Firmware: ___Hardware: ___ Documentation: ___

Other: _______________

CHANGE TYPE:

New Requirement: ____________ Requirement Change: __________

Design Change:____

Other: ____

REASON:

Legal: ___Market: ___ Performance: ___ Customer Request: ___

Defect: ________________

Other: _________________

PRIORITY:

Emergency: ________ Urgent: _________ Routine: _________

Date Required: ____/____/____

CHANGE DESCRIPTION: *(Detail functional and/or technical information. Use attachment if necessary.)*

Attachments: Yes / No

TECHNICAL EVALUATION: (Use attachment to explain changes, impact on other entities, impact on performance etc.)

Received By:________________________Date Received: ___/___/___

Assigned To:________________________Date Assigned: ___/___/___

Type of Software/Hardware/etc.

Affected ____

Modules/Screens/Tables/Files Affected:

____

APPROVALS: Change Approved: ______ Change Not Approved:

____

Hold (Future Enhancement): ________________________________

1. Approved By::____

Signature ______________________________Date: ____/____/____