KUMASI TECHNICAL UNIVERSITY

ICT SECURITY POLICY

(ICT-SP)

October, 2020

Table of Contents

1.0 Introduction

1.1 Preface

Subject: These security policies are provided for all members of the University community to establish requirements for each individual to follow in order to safeguard the University's academic and administrative information resources.

Procedures: IT Security Guidelines, ICT Directorate web pages, Network Host Security Standard (access limited to System Administrators through ICT Directorate Helpdesk)

Related University ICT Policies:

i. ICT Resource Use Policy (I-RUP)

ii. Hardware Replacement and Maintenance Policy (HRMP)

iii. Software Management and Usage Policy (SMUP)

iv. Backup Policy (Disaster Recovery Plan)

1.2 Scope

This policy covers the security management of the infrastructure of the ICT of the Kumasi Technical University. It is a working document for the ICT Infrastructure Unit of the ICT Directorate.

Kumasi Technical University conducts significant portions of its operations via wired and wireless computer networks. The confidentiality, integrity and availability of the information systems, applications, and data stored and transmitted over these networks are critical to the University's reputation and success. KsTU systems and data face threats from a variety of ever-changing sources.

1.3 Purpose

The main purpose of this policy is to reduce and, if possible, eliminate cyber risk by detecting, preventing and mitigating all cyber threats to the institution. Other purposes include:

i. To enable all members of the University community to achieve their academic or administrative work objectives through the use of a secure, efficient, and reliable technology environment;

ii. To protect academic, administrative, and personal information from current and future threats by safeguarding its confidentiality, integrity and availability;

iii. To establish appropriate policies and procedures to protect information resources from theft, abuse, misuse, or any form of significant damage while still enabling community members to fulfil their roles;

iv. To establish responsibility and accountability for information technology security within the organization;

v. To encourage and support management, lecturers, non-teaching staff and students to maintain an appropriate level of awareness, knowledge and skill to enable them to minimize the occurrence and severity of information technology security incidents;

vi. To ensure that the University is able to effectively respond to, contain, and address significant security incidents, while being able to continue its instructional, research, and administrative activities.

1.4 Policy Statement

Information and communication system resources are essential assets of KsTU. The entire community is responsible for ensuring that computing and communication facilities are used in an effective, efficient, ethical and lawful manner.

While these policies identify many roles and responsibilities for safeguarding information resources, they cannot possibly cover every situation or future development. Therefore, this is to be considered a “living document” which will be modified or changed as needs require. It will be reviewed on, at least annual basis to ensure compliance with current rules and regulations.

1.5 Applicability

This policy applies to vendors, volunteers, contractors, consultants and any other person having access to KsTU institutional information or technology resources.

This policy applies to all electronic information system resources of KsTU, including technology hardware and software owned, leased, or licensed. This includes hardware and software used to process, store, retrieve, display and transmit electronic representations of data, voice, and video content.

Personally owned equipment is also covered if it is used to process KsTU institutional information or is connected, directly or indirectly, to the KsTU network. The University will not access or modify software or information stored on personally owned equipment without permission of the owner; however, access to the KsTU network may be denied or limited unless these policies are complied with fully.

2.0 Security Roles and Responsibilities

2.1 Risk Management Team

According to experts, cyber security is not an IT problem but rather a business concern. In view of this fact, a risk management team of competent, knowledgeable and dedicated people should be constituted.

2.2 Risk Management members

The risk management team shall comprise the following:

i. Director of ICT – leader

ii. Head of ICT Infrastructure Unit – member

iii. All Heads of ICT Units – members

iv. Computer Science Dept. Rep (ICT Security)

v. Quality Assurance and Planning- Rep

vi. Systems Auditor (Audit representative)

vii. Deputy Director of Finance

viii. Finance Directorate Rep

ix. Deputy Director of Works and Municipal Directorate

x. Procurement Officer

2.3 Roles and Responsibilities

The roles and responsibilities of the risk management team include but not limited to the following:

i. See to the enforcement of this policy.

ii. Provide technical support to ICT implementation committees.

iii. Review and make recommendations to this policy periodically (preferably annually).

iv. Measure the deliverables of all ICT projects.

v. Ensure the availability and suitability of all ICT infrastructure equipment.

2.4 Standards

KsTU's technology environment is a shared and limited community resource subject to both ICT Directorate and unintended abuse. Computing systems and other specialized devices have the potential to introduce security risks, especially when they are attached to a communications network. To mitigate risk, standards for managing and securing applications, work stations, servers, network devices, and third-party services have been developed.

As new equipment or applications are introduced into the environment, a risk assessment shall be conducted to ensure compliance with these standards prior to use or network attachment. The risk Management Team shall periodically conduct compliance reviews and test for vulnerabilities on all systems and networks to ensure that systems and applications are updated as new vulnerabilities are discovered and threats revealed.

3.0 Requirements

3.1 General

3.1.1 Network Usernames and Passwords

Logical access controls can prevent or discourage unauthorized access to information resources and help ensure individual accountability. Therefore, individual users must be identified and granted appropriate levels of access to Network devices by means of a unique username coupled with a password or some other form of secure authentication process. A unique username is required to provide for individual accountability in audit logs, etc. For this reason, generic or group IDs are not permitted.

Default manufacturer passwords on all systems and devices must be changed. Replacement passwords must be composed in accordance with the following naming convention:

i. Passwords must be at least eight (8) characters in length and be composed of both letters and numbers.

ii. Passwords may not be repeated within the past year.

iii. Passwords should be changed frequently, but are required to be changed every ninety (90) days.

3.1.2 Secure Verification of Username and Password

Under some conditions, it is possible to eavesdrop on network traffic. For this reason, all Username and password authentication procedures (accept one-time password authentication systems) must use an encryption mechanism. This means that only encrypted versions of popular e-mail, file transfer, and other network access programmes may be used.

3.1.3 Third-Party Services

When a third-party is used to provide services or to store data, security requirements should be considered and made part of any contractual agreements. Such vendor agreements must include appropriate safeguards for the security of the University's information and resources and audit rights. Vendors and independent contractors (hereinafter collectively referred to as "Vendors") may only have access to the minimum necessary information to perform the tasks for which they have been retained. Vendors must comply with all applicable KsTU policies and practices. Vendor access must be uniquely identifiable. Major vendor work activities should be logged and include such events as personnel changes, password changes, milestones reached, deliverables, and arrival and departure times.

Upon departure of a vendor employee, the vendor must be required to return or destroy all sensitive information, and surrender all KsTU identification badges, access cards, equipment and supplies immediately.

3.2 Hardware

3.2.1 Device Registration

The ICT Infrastructure Unit shall ensure that all devices are registered using its MAC and IMEI addresses.

3.2.2 Assignment of Network Identifiers

In order to ensure reliable network operations, all devices must be configured to accept the assigned Internet Protocol (IP) address, KsTU-generated identifying name, and other network parameters which are automatically assigned each time a network connection is established. The use of permanent network identifiers is restricted to the ICT Directorate.

3.2.3 Equipment Disposal

Sensitive University academic or administrative information is likely to be present on storage media associated with obsolete or surplus equipment intended for disposal. University-owned technology equipment must therefore be disposed of by the University's asset disposal committee in conjunction with the Risk Management Team.

3.2.3 Server Registration

If a network device provides services to multiple users, there are additional registration requirements which need to be set. Allowing outside systems to initiate connections to the University system increases the risk to threats from the Internet. Outside systems cannot successfully achieve such connections unless the University system is publicly addressable, i.e. it has a Public Internet Address. Publicly accessible systems must be registered with the ICT Directorate.

3.2.4 Security Configuration

The ICT Infrastructure unit and the risk management team are responsible for ensuring the security and safety of the publicly accessible systems in the institution. They will develop and administer security configurations as well as ensures that the Network and Host Security Standard referenced in this policy are met.

3.3 Software

3.3.1 Anti-Virus Software

Computers infected with viruses or malicious code can jeopardize information technology security by contaminating, damaging, and destroying data. Therefore, anti-virus software must be installed and updated regularly. The University has licensed anti-virus software for use by every KsTU user.

3.3.2 Firewall Software

The infrastructure unit staff and the risk management team shall ensure that all personal computers must use firewall software configured according to KsTU guidelines.

3.3.3 Licensed Software

Software installed on any TUK computer system must be legally licensed accordingly with the software management and usage policy.

3.3.4 Software Patch Updates

All currently available security patches for operating systems and application software must be installed. Software for which security patches are not routinely made available should not be used on the KsTU network.

3.3.5 End Point "Health Check"

All computers connected to the KsTU network are required to undergo an automated evaluation to determine if certain software settings and applications are correctly installed and operational. As a result of this evaluation, the user may be required to install new software or reconfigure existing software before unlimited network access is granted. Access to Internet resources needed to accomplish any required upgrades will be permitted. The University will not access or modify software or information stored on personally owned equipment without permission of the owner; however, access to the KsTU network may be denied or limited unless these policies are complied with fully (Refer to the software management and usage policy for additional information).

3.3.6 Secure Data Transmission

Encrypted communication channel must be used for staff working at off campus location and remotely connecting to systems on the KsTU network, in order to protect the confidentiality of Usernames, passwords, and University records containing personal, confidential, or legally protected information. This is also necessary when using the on-campus wireless network.

A general-purpose encrypted communication link can be accomplished through the use of "virtual private network (VPN)" technology. By accessing the KsTU network via this special web interface, the security requirements of this section will be met. When using KsTU's VPN technology with personal equipment, users must understand that their machines are acting as an extension of KsTU's network, and as such are subject to the same rules and regulations that apply to KsTU-owned equipment.

3.3.7 Secure Data Storage

Sensitive personal information must be stored within University systems using an approved method of encryption to help secure the data in the event of unauthorized access. This requirement is especially important when information is stored on portable devices.

4.0 Security Monitoring

4.1 Network Monitoring

The Network Engineers in the ICT Infrastructure Unit of the ICT Directorate shall design, configure and deploy a standard network monitoring system to keep the institution's network free from network intruders.

4.2 Penetration Testing

The Network Engineers shall carry out penetration testing on the institution’s network at least once every year to plug all unused ports to prevent network intrusions. This can be done in-house or with qualified external consultants.

4.3 Systems Logs Monitoring

The Infrastructure unit staff will review all systems logs daily, weekly or monthly to help them trace back the source of cyber-attacks.

This could be done as follows:

i. Confidential Computers – based on user request and during investigations

ii. Servers – daily, weekly

iii. Routers – continuous (online), daily

4.4 Physical Security

4.4.1 Server Room Management

The Head of the ICT Infrastructure shall appoint a staff under his unit to rotationally or permanently stay at the server room to physically monitor the devices at the server room. The monitoring includes checking the physical conditions of the devices at the server room. Readings for temperatures, fire control systems, generator fuel, visibility status, cable and devices health, and alarms are to be taken at regular intervals and results plotted on graphs to detect changes and prescribe remedies for them.

4.4.2 Wireless Access Point Monitoring and Protection

The network Engineers shall monitor all wireless access point (WAP) online in real time to reduce downtimes. They shall also check physically the conditions of their position in terms of directions and signal strength.

Recommendations shall be made to the Director of ICT through the head of the ICT infrastructure unit to make the wireless connection on KsTU campus efficient and effective.

4.4.3 Communication Links Monitoring and Protection

It is the duty of the ICT Infrastructure Unit to physically monitor all physical conditions of communication links, including cables, trunkings, satellite dishes, radio devices, poles, and mast

5.0 Data Backup and Recovery

Production servers and computers offering shared network resources shall be backed up regularly to provide protection against hardware failures and other disasters.

Individual computers shall not be backed up by ICT Directorate. Education shall be given to individuals to back up their critical data.

A comprehensive business continuity plan (backup policy) to manage the institution's data backup and restoration shall be implemented and documented.

6.0 Security Awareness and Training

It is essential that all aspects of information technology security, including confidentiality, privacy and procedures relating to system access, be incorporated into formal student, lecturers and non-teaching staff orientation procedures to educate the members of the University community.

The ICT Directorate shall hold semi-annual meetings with departmental technical partners at which current and pending security issues and new potential risks would be discussed and mitigation strategies shared.