SECURITY POLICY

FOR

UGANDA INSTITUTE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

May 2019

BY

OYEE JAMES
+256773895415
engjames256@gmail.com

Introduction

This document specifies the conditions that must be followed to ensure security at Uganda Institute of Information and Communications Technology. The document covers both physical and digital items owned by the institute. The document covers both digital and physical items owned by the institute. It also looks at the steps that may be taken to enforcement of this policy and the revision history.

Digital Security Policy

1. WIFI

- The administrative username and password for the router shall be changed after every 3 months.
- All WiFi internet users shall register the MAC Address of their devices with the IT office in order to be connected.
- All wireless hardware implementation shall utilize WiFi Certified devices that can be configured to use the latest security features.
- All wireless access points connected to the network shall be registered and approved by Uganda Institute of Information and Communications Technology.

2. CCTV

- The CCTV camera of the institute shall be kept working everyday and maintenance must be carried out every 3 months.

Physical Security Policy

1. Gate

- The institute should have only one gate used by students, visitors and all employees plus cars.

2. Guards

- Guards shall wear their uniforms every time they are on duty.
- Guards shall check all the cars accessing the school and any lagage the may carry.
- Guards shall check everyone accessing the school and any accessories they may possess.
- Guards shall be equipped with all the necessary tools for them to operate like metal detectors.

3. Parking

- Staff of the school should have a seperate parking space from visitors to the institute.
- Parking should be allocated for staff members to park indicating the titles of the person allocated to.

4. Compound

- Everyone must assemble at the assembly point marked on the compound incase of any danger like fire outbreak.

5. Classroom Block

- All classroom doors and windows must be properly locked after the last lecture of the day.

6. Laboratory (Electrical and Computer)

- Bags shall not be allowed in the library.
- Repair and Maintenance should be carried on the computers to assess ensure their status every 3 months.
- The laboratory should have only one entrance and students should leave their library card with the liberian before access.

7. Library

- Bags shall not be allowed in the library.
- The library should have only one entrance and students should leave their library card with the liberian before access.

8. Administration Block

- The administrative block should have only one entrance and only authorised visitors should be allowed to access respective offices via intercom.
- Windows and doors must be closed off before leaving class.

9. Student's Hostel

- Students must report any stranger or suspicious person in their residence to the authorities in charge as soon as possible.
- You should never lend you key to any one.
- A student should know all individuals they are letting in before they open the door.

Enforcement

- Police and local authority may be involved to handle violations to this policy.
- Any one found to have violated this policy may be subjected to disciplinary action up to or including termination of employment.
- The institute shall enforce this policy through various methods, including but not limited to periodic walk throughs, video monitoring, internal and external audits.

Revision History

May 2019, Policy Developed by Oyee James