UGANDA MANAGEMENT INSTITUTE
MOBILE DEVICE GUIDELINES

1. Introduction

In line with the Policy statement, section 2.1 of the Institute's Information Security Policy, mobile devices such as Laptops, tablets and smart phones are part of computer equipment that are subject to secure control to protect them from accidental or intentional loss, both within the Institute and externally. Mobile devices are versatile and portable and are at greater risk of theft, both for the device itself and the data/information contained therein.

These guidelines are intended at ensuring that a person allocated a laptop, tablet or other mobile device understands the associated risk and assumes the appropriate level of responsibility for the Institute's property. These guidelines are inline and in addition to those already mentioned in Information Security Policy, the Information Security Operations Manual which covers Security Controls for ICT Assets and the Human Resource Manual covering the use of Institute Property.

2. Scope

These guidelines cover all employees (full time, temporary or contract staff) who use mobile devices provided by the Institute.

3. Security Risk

Mobile devices are vulnerable to loss and theft due to their portability and small size. Any loss may lead to undesirable costs which are not limited to asset value, but loss of productivity, data replacement, and the like. Mobile device may be targeted either on campus or off campus or while in transit. Thefts may be either for resell at a quick profit or stolen for the data they may hold. Such information, if revealed, may cause embarrassment, have a negative impact on the reputation of the Institute.

4. User Responsibility

4.1. General rules

i. Mobile devices must be protected by a password or pin code and Users must take shared responsibility for the security of their equipment.
ii. Any mobile device(s) issued to a staff remains the property of the Institute and is intended for official use only.
iii. Upon leaving employment or changing to a new role where the mobile device is no longer required, it must be returned to ICT Department. The supervisors/ line managers will ensure that the equipment is returned to the ICT Department.
iv. Before installing software onto mobile devices, staff should contact the Head ICT Department for authorisation and where possible, installations should be carried out by ICT technical staff.
v. Use of unlicensed software is illegal and puts the Institute at significant legal risk.
vi. Users are specifically prohibited from changing security settings or amending configuration files on mobile device issued to them. This includes disabling passwords, pin codes and any installed security programs.
vii. In the event that a mobile device is either lost or stolen, the user must notify the police, Supervisor, Human Resource Manager or any other appropriate authority. It is the User's responsibility to obtain a police report and to inform both their Supervisor and the ICT Department as soon as possible after the event.
viii. Loss of either device or data or information caused by either negligence or disregard to the recommendations made in this document and overall information security policy shall be the sole responsibility of the user.

4.2. Physical Security

Apart from the financial cost associated with replacing a stolen mobile, device there are associated hidden costs which include loss of productivity, data replacement, and so on. All Institute mobile device users are encouraged to take the following physical security measures to prevent lost or theft of their devices and sensitive information.

i. Mobile devices must not be left in full view in a vehicle even for a short period of time.
ii. Mobile devices must never be left unattended in public places even for a very short period of time.
iii. Mobile devices must not be left in a vehicle overnight, even in a locked boot.
iv. When a mobile device to be left un-attended for an extended period of time, it must be locked away or if possible, secured with a cable lock or deposited for secure custody.
v. When travelling mobile devices must always be carried in the cabin with the User and within their view.

4.3. Access control and Data protection

i. All users must use a password or pin code in order to protect information on a mobile device and screen displays must be locked with the password protected screen saver when left unattended.
ii. When working in public places such as restaurants, hotel lobbies, on buses or aircraft, care should be taken to prevent others from being able to view potentially sensitive information. Loss of sensitive data or information could potentially damage the Institute.
iii. When not connected to the Institute's network, Users should save all work related documents to an appropriate local folder and any changes made to files while not connected should be copied back to the normal storage location at the next opportunity.
iv. Take care when connecting either cables or accessories to the mobile device as wrong connections can easily damage the device.
v. Turn the mobile device off and put it in an appropriate carrying case when travelling.
vi. Keep all drinks and any other liquids away from your mobile device. Any spillage on the device can result in data loss and expensive repairs.
vii. Avoid turning off your mobile device (especially laptops and tablets) when the hard disk light is on, this can result in data corruption and / or data loss.
viii. Don't subject the mobile device to extreme temperature changes. For example do not use or store them near radiators or fan heaters.

5. Violations and Penalties

Violation of these guidelines may result in disciplinary action as specified in section 7 of the Institute's Information Security policy; that is, violations are subject to sanctions prescribed in, but not limited to, the following policies: Human Resource Manual, Computer Misuse Act, 2011, and The Uganda Public Service Standing orders.

6. Device Details:

Device Type: ____________________Model: ______________________S/N: ______________________

Engraved No:___________________IMEI No: __________________ Wi-Fi: ____________________

I, _________________________________, the undersigned, agree to comply with the above guidelines.

Signature: _____________________________ Date: _________________________________