Uganda Management Institute

Information Security Policy

Document code/no:

Date approved: 4th April 2016

Foreword

Campus networks and computing technologies form a complex framework that involves business processes, participants, faculty and administrative staff, all working together to provide institutional capacity to securely process, store and transmit information in support various academic and administrative functions. The selection of appropriate security controls is an important task that can have major implications on the operations and assets of an institution.

This Information Security Policy has been formulated to guide the context within which information security is ensured within Uganda Management Institute (UMI). It covers the identification, promotion and appropriate utilization of Information and Communication Technology at Institute to ensure that ICT applications are well integrated into the planning, implementation and managing of Institute business.

The Policy aims at enabling the Institute achieve its vision of being a World Class Management Development Institute through supportive ICT interventions that address and ensure confidentiality, integrity, availability, authenticity and compliant use of information resources. This implies addressing any ICT dimensions that includes infrastructure, systems, content, programmes and human resource development. Several technological, institutional and structural changes will be required to implement this Policy with a view of addressing any identifiable gaps and take into account emerging ICT-related issues relevant to the realisation of the Institute and National visions.

The Information Security Policy will enable the Institute achieve excellence in its academic, research, consultancy and administrative services. The Policy is organized around four core sections; *the situational analysis and policy challenge, Policy Statement and Scope of application, Policy Framework, Implementation, roles and responsibilities*. These broadly fall under ICT infrastructure and services, integrated management information systems, ICT security, Governance, Communication and Control, Email and Website management, Social Media control, Sustainability of ICT, as well as Policy Monitoring and Evaluation.

It is worth mentioning that the development of this policy has involved a number of stakeholders and I would like to thank them all for their invaluable contributions. It is my view that the shared objectives of this Policy will be realized only when the different stakeholders play their respective roles effectively.

Dr. James L. Nkata
Director General

Table of Contents

Acronyms and Abbreviations

CD-ROM	-	Compact Disc Read-Only Memory,
CD-RW	-	Compact Disc - Rewritable
DVD	-	Digital Versatile Disc
ISO	-	Information Security Officer
ISP	-	Internet Service Provider
ICT	-	Information & Communication Technology
IAO	-	Information Asset Owner
ICTSC	-	Information & Communication Technology Steering Committee
LAN	-	Local Area Networks
PABX	-	Private Automatic Branch Exchange
PC	-	Personal Computer
RAS	-	Remote Access Service
H/IAD	-	Head Internal Audit Department
HRM	-	Human Resource Manager
PDA	-	Personal Digital Assistants
PPDA	-	Public Procurement and Disposal Act
SA	-	Systems Administrator
SM	-	Social Media
TO	-	Technical Officer
UPS	-	Uninterruptible Power Supply
WAN	-	Wide Area Networks

Definitions of Key Concepts

Concept	Definition
Access	Means gaining entry to any electronic system or data held in an electronic system or causing the electronic system to perform any function to achieve that objective;
Application or Computer application	Means a set of instructions that, when executed in a computer system, causes a computer system to perform a function and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system;
Bandwidth	Expressed in a range of frequencies using hertz as the unit of measurement; also called analog capacity
Browsers	These are computer applications that are used to access information or resources on the world wide web

Concept	Definition
Building backbone	This is network infrastructure that connects LANs within a building
Computer	Means an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices;
Computer System or System Resources	These are resources involved in the sharing and accessing of electronic resources. This includes, but is not limited to, applications, computers (desktops, laptops, servers), PDA's (Palms, Pocket PCs), networking devices (routers, switches) and printers.
Contractors	These are service providers, either as groups or individuals to either design, develop and/or manufacture one or more products or service
Data	Information manipulated inside the computer represented in electronic form of bits and bytes.
Database	A collection of related data stored in one or more computerised files in a manner that can be accessed by users or computer programs via a database management system
Ethernet	most commonly used protocol designed to change the packets into electrical signals that can be sent out over the wire
Firewall	A barrier between a network and the Internet through which only authorized users can pass; set of security policies to screen incoming and outgoing messages; also used to isolate one part of a network from another
Floppy disc	This is a storage device for computer information.
Information	includes data, text, images, sounds, codes, computer programs, software and databases;
Information Asset	An identifiable collection of data stored on ICT Assets and recognised as having value for the purpose of enabling the Institute to perform its business functions.
Information System	A system for generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system;
Information Asset Owner	This is an individual or department that is responsible for the information security of a particular Information Asset.
Information Technology	This includes computers, ancillary equipment, software and firmware and procedures, services and includes any equipment or Interconnected system or subsystem of equipment, which is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.
Interface	Point in the system where the rules, control codes, formats, and information direction (as dictated by the protocol) are implemented
ICT Asset	All applications and technologies that are owned, procured and /or managed by the Institute. These include desktop and productivity tools, application environments, hardware devices and systems software, network and computer facilities, and management and control tools.

Concept	Definition
Local Area Network	Network that operates within a small geographic area, usually within a building, office, or department
Leased lines	Another name for private lines, dedicated lines, or permanent circuits that are provided by telecommunication companies to enable the transfer of electronic data.
Metropolitan Area Network	This type of network connects sites in and around a large city
Manager	Managers have management or supervisory responsibility, including Directors, Deans, Heads of Department, Managers, and Supervisors, as well as others with similar responsibility.
Operating system	interface between the application (word processor, spreadsheet, etc.) and the computer hardware
Optical media	This is optical storage device read by lasers and can hold up to 700 megabytes of data or more, such as CD-ROM (compact disc read-only memory), CD-RW (compact disc - rewritable), DVD (digital versatile disc)
User or End User	A user is anyone who uses a computer resource
Participants	In the case of the Institute, the term “Participant(s)” may refer to Students that attend training programmes at the Institute
Program or Computer Program	This means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.
Social media	This is media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques using the internet.
Workstation	This means equipment such as personal computers, portable computers, servers or other data processing desktops and hand held computers.

1.0 Situational Analysis and Policy Challenge

1.1 Introduction

This Information Security Policy provides the context within which information security should be ensured within Uganda Management Institute. It is designed to support the overall ICT Strategic Plan of the Institute and is based on; the International Standard ISO/IEC 27001 for Information Security Management Systems, the National Information Technology Policy, 2012, National Information Security Policy, 2014 and the Computer Misuse Act, 2011.

This document is intended to act as a point of reference for information security related policies and standards within the Institute. It is to provide a "baseline" to which all areas of the business must adhere to with regard to information systems.
All forms of information need to be protected, regardless of the medium used for communication or storage. All the Institute's employees, participants and contractors are responsible for protecting this information. The Institute's information processing resources should be used only for designated business purposes. These resources should not be used for such purposes as personal benefit, entertainment, or amusement.

To accomplish this, an Information Security Operations Manual has been developed with guidelines and procedures for protecting information from accidental or intentional unauthorized modification, destruction, and disclosure. The Operations Manual is supposed to be followed by information system users on a day-to-day basis.

1.2 Background

Information is critical to most of the functions of an education Institution, whether for teaching, research, administration, employment or funding. The effective operation of all those functions depends on reliably accurate information being available when it is needed by those who are authorised to see it, and is not disclosed to those who are not authorised to see it. These factors - accuracy, availability and confidentiality - are all components of information security. This Policy document covers the key requirements to achieve the necessary level of information security, concentrating almost entirely on people, processes and policies, and not limited to computers or networks.

This policy is driven by the desire to achieve the Institute's strategic objective of strengthening capacity of the administrative support functions to facilitate effective and efficient delivery of UMI services. The main focus of this strategic objective is to;

i. Build a comprehensive and integrated ICT infrastructure
ii. Promote utilization of ICT as a delivery mode in UMI services

1.3 Existing Legal and Institutional Framework

Apart from the National ICT policies (Nation IT Policy 2012, Computer Misuse Act 2011, National Information Security Policy 2014,) and ICT best practices that the Institute can follow, there are no specific internal policies or guidelines that promote and ensure secure utilisation and development of ICT within the Institute. This situation has a negative influence on the secure utilization and development of ICT related services and technologies within the Institute.

In terms of Institutional framework, the Institute established an ICT Steering Committee (ICTSC) as an executive organ that steers and oversees the development of ICT within the Institute and is responsible for information security management.

Therefore, by developing and establishing this policy, the ICTSC will be addressing the legal aspects and at the same time meet one of its mandates of ensuring information security within the Institute. This policy identifies the key actions parties, their roles and responsibilities towards the implementation of the policy.

1.4 Issues: Core and specific

In the developing this policy the Institute is looking at the following core issues;

a) To safeguard the integrity of information assets at the Institute and elsewhere,
b) To ensure that use of electronic resources complies with the Institute policies,
c) To protect the Institute against unnecessary ligation,
d) To ensure continued availability and growth of information systems,

The specific in this policy are mainly concerned with; *Personnel Security, Physical Security, Workstation Security, Security Control of Information Assets, Communication and Operation Management, System Access Control, Website and E-mail Security, Social media, roles and responsibilities, Network Monitoring and Business Continuity.*

2.0 Policy Statement and Scope of Application

2.1 Policy Statement

The Institute's Information Security Policy is in respect of policy, planning and governance, asset management, human resources management, physical and environmental management, communications and operations management, access management, system acquisition, development and maintenance, incident management, business continuity management, and compliance management.

While computerised information assets and computer equipment shall be provided to employees, participants and/or third parties to enable them carry out their duties satisfactorily, these assets;- information and physical equipment;- shall be subject to secure control to protect them from accidental or intentional loss, unauthorised manipulation or disclosure both within the Institute and externally.

The policy recognises that effective information security involves the cooperation of all the different units across the entire Institute and depends on responsible use of the Institute's IT systems by its users

2.2 Scope of policy application

The policies and guidelines contained herein apply to all UMI Study Centres, Schools and Departments that have access to it's computerised information systems. Information security applies to all employees, faculty, participants, visitors, guests and all others who directly or indirectly use or support the Institute's ICT services and information.

2.3 Guiding Principles

This Information Security Policy, supporting documentation and procedures, provide a framework to implement best practices for information security within the Institute. The development and management of this policy follows the guiding principles below;

a) **Top Leadership Commitment:** The Institute is committed to protecting the confidentiality, integrity and availability of its information and hence will have its information and systems secured and with restricted access.
b) **Business focus:** Information technology resources are intended to support and achieve the Institute's vision, mission, academic and administrative activities.
c) **Accountability:** The Institute and its faculty, staff and participants are accountable for compliance with the information security policy and other applicable laws.

d) **Teamwork:** Successful implementation of this policy will be realized only when the different stakeholders play their respective roles effectively and support one another.
e) **Complimentary legal framework.** This Policy complements and supports other Institute policies that protect the Institute information assets and resources including, but is not limited to, Staff Regulations, Computer Misuse Act, 2011, the National Information Security Framework, 2014 and The Uganda Public Service Standing orders.

2.4 Policy Objectives

The policy objectives are aimed meeting the Institute's strategic objective of strengthening capacity of the administrative support functions to facilitate effective and efficient delivery of UMI services. The overall objective of this policy is to protect information assets and ensure business continuity by preventing and minimizing the impact of security incidents. More specifically, the policy will:-

a) **Promote confidentiality:** protecting sensitive information from unauthorized disclosure or interception.
b) **Enhance integrity:** safeguarding the accuracy and completeness of information and computer software.
c) **Ensure availability:** ensuring that information and vital services are available to Users when required.
d) **Ensure authenticity:** ensuring confidence that information was sent by the originator.
e) **Ensure Compliant Use:** meeting legal and contractual obligations.

This Policy document contains aspects relating to the above statement and has been duly approved and communicated to all users of computerised information systems of the Institute

3.0 Policy Framework

3.1 Personnel Security

This is one of the most critical areas of data security since employees are ultimately responsible for controlling the dissemination of confidential information and data security measures rely on the honesty and capability of individuals. Consequently, the management of data security should involve consideration of a number of personnel issues that shall include the follow;

a) The Institute will ensure that employees are provided with training to encourage adherence to this policy and Staff Regulations.
b) Upon termination of employment or changes in responsibilities, the Institute shall take appropriate measures to ensure that the access controls are changed to reflect the changes in responsibilities.
c) All staff, participants contractors and other stakeholders of the Institute with access to ICT infrastructure and information will sign confidentiality agreements and will abide by the rules as stipulated in the Staff Regulations.

3.2 Physical security

Physical security of computerised facilities is necessary for two main reasons:-

a) to prevent unauthorised access to and use of computer equipment,
b) to ensure that computer equipment is adequately protected against natural hazards, theft, and damage.

These facilities include computer rooms, network control centres, and other related areas. It is imperative to note that the greatest threat to Physical security depends mostly on users.

UMI will physically restrict access to components of the data processing equipment including computers, peripherals, terminals, communication equipment and other related equipment.

UMI shall provide network security resources at a level that is appropriate for the nature of the data transmitted. The administrators will ensure that access to data transmissions is restricted to authorised personnel internally and will control the flow of data between the Institute's private network and external public networks through the use of secure communication devices.

3.3 Network Security

The Network encompasses wired and wireless network connections in offices, computing labs, student resource centres, libraries, conference rooms, classrooms, and

other Institute locations. It includes connections to external networks such thee national backbone, Internet service providers, and international research and educational networks as well as the Internet. All computing resources are interconnected creating the need for an adequate level of security exists over the entire data network.

The growth in the use of communications systems has increased the significance of network security in computer systems. The need to ensure that transmitted data is given appropriate protection against potential threats should be considered by Management. Controls are required to ensure that messages are not corrupted and unauthorised access to the systems is not gained via the communications systems.

UMI shall provide network security resources at a level that is appropriate for the nature of the data transmitted. The administrators will ensure that access to data transmissions is restricted to authorised personnel internally and will control the flow of data between the Institute's private network and external public networks through the use of secure communication devices.

3.4 Workstation Security

All users requiring access to the information systems will be provided with a workstation in order to be able to carry out their duties. At any time these workstations hold Institute confidential data as well as being gateways to the Institute network. It is therefore important that there is adequate level of security over workstations.

UMI shall provide users with workstations in order to enable them access the Institute's network as well as carry out their duties. Workstations not owned by the Institute will not be allowed to connect onto the Institute's network unless either a User seeks permission or the appropriate authentication has been met. All persons granted access must not use Institute workstations to engage in any activity that is either illegal under national or international law, or is in violation of the Institute's Information Security policy.

3.5 Security Controls for ICT Assets

It is important that ICT Assets are not confused with other Institute Assets such as classroom furniture, buildings. Information security control measures require that special attention is given to the management of ICT Assets other than for purposes of property control and tracking.

All employees, participants and contractors that have access to Institute information systems must adhere to the ICT Asset control guidelines established by the Institute in order to protect network resources, ensure data integrity, control information systems and Assets. This may involve support and collaboration with vendor where applicable.

The guidelines must define what must be done when a piece of ICT Asset is either moved from one location to another or from one user to another, or installed on another device. Also to be defined are the details to be tracked using an asset tracking database for all ICT Assets and should covers the possibility that data on an Asset moved between secure facilities may be sensitive and must be encrypted during the move.

These guidelines are in addition to those defined in the Finance Policies and Procedures Manual regarding Fixed Assets. The guidelines will not only enable ICT assets to be tracked with regard to their location and persons using them but will also protect any data being stored on those assets. The Institute must therefore establish guidelines for tracking and controlling ICT Asset in order to protect the data contained within.

3.6 Communication and Operation Management

Management of Information Systems within the Institute shall strive to ensure correct and secure operation of all ICT services as a whole. This covers change management, incident management, virus control, and related disciplinary measures.

In order to minimise the corruption of information systems, the Institute will ensure that strict control is exercised over the implementation of changes. The change control procedures shall ensure that information security and integrity are not compromised, and approval for the change is obtained.

3.7 System Access Control

System access controls are required to ensure that computer users only access data to which they have been authorized. The application of this ("logical") access security will help to reduce unauthorized access to information systems or alteration of data. Access control software provides protection over access to both application systems and system resources. The controls should enforce segregation of duties between incompatible functions.

UMI shall protect all its information system from unauthorized modification, disclosure, or destruction and assure that the systems are accurate, trusted and available. Access to information systems shall be restricted to those people who need the information for their business function.

3.8 Website Security

The Institute has developed this website security policy to document and communicate its commitment to safeguarding information about website visitors and to secure information on the website. It describes the information that may be collected and the website security measures. However it does not cover links to other websites that may appear on the Institute website. When you visit links to other websites, you should abide by the website security policy there.

The Institute respects the privacy of all website visitors and is committed to ensuring confidentiality of their information and will implement the necessary internal controls to protect this information. However, while the Institute does not actively share information, it may in some cases be compelled by law to release information gathered on the Institute's website servers.

3.9 E-Mail

This policy provides users with guidelines for permitted use of its email system and ensures that the system is secure from unauthorized access. It covers email either coming from **umi.ac.ug** email address space or going to all UMI computers, servers, laptops, paging systems, mobile devices and any other resources capable of sending or receiving e-mail.

Email correspondence is considered an official form of communication within Institute and that the Institute owns the system, messages generated or processed by the system including backup copies, and the information contained therein. Although users receive an individual email account, email and its resources remain the property of the Institute.

All official communication via e-mail should either be forwarded or communicated to the appropriate office(r) and a copy of the e-mail and/or attachment(s) appropriately filed.

3.10 Social Media

Social media gives the faculty, staff and participants of the Institute an opportunity to share information and knowledge and to foster learning, innovation, collaboration, and research. The information may be further shared and exchanged almost instantaneously with other users all over the world. This capability brings with it the potential to impact the reputation of the Institute and its representatives.

In order to manage this impact, the Institute requires that all social media accounts used and management on behalf of the Institute be consistent with the core values of the Institute, applicable laws and promote thoughtful discourse on appropriate matters. Institute staff and participants represent not only themselves, but also other UMI participants, administration, faculty, staff, and the Institute as a whole. Therefore the Institute shall provide guidelines to enhance and protect both personal and professional reputations of its participants, employees, and third-party organizations participating in online social media as well as the institute's reputation as a whole.

The social media guidelines will apply to all social media activities undertaken by Institute staff, participants, and other third parties acting on behalf of the Institute, its

schools and departments using social media accounts on platforms such as Facebook, Twitter, LinkedIn, YouTube, etc.

3.11 Disaster Contingency Planning

To ensure continuity of data processing following a disaster or system or transaction failure, a full copy of required documentation, systems software, applications software and production data, including transaction logs, must be available to allow restoration of lost or damaged data.
In addition, adequate procedures should be in place to allow the organization to re-establish customer and business services in the event of a disaster.

The Institute will have a disaster contingency plan to ensure that its critical business activities are maintained and restored as quickly as possible following any major disaster or failure that affects essential services or facilities.

4.0 Implementation, Roles and Responsibilities

4.1 Success factors

In order to successfully implement and manage information security within the Institute, the following must be addressed;

a) A management framework must be established to initiate and control the implementation of information security within the Institute.
b) Management must actively support security within the Institute through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.
c) All information security responsibilities must be clearly defined and done in accordance with this policy.
d) A management authorisation process for all information processing facilities must be defined and implemented.
e) Information security management and its implementation must be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

4.2 Action Parties

All managers, at every level, are directly responsible for ensuring that all employees, participants and contractors are aware of their obligations and responsibilities to safeguard the Institute's information assets.

All users of the Institute's computer resources have a responsibility for protecting the security and integrity of information and equipment.

4.3 Policy Implementation and Coordination

This policy adopts the ISO/IEC 27001 Plan-Do-Check-Act (PDCA) continuous improvement model to structure all security governance processes. It focuses on all the activities required to manage a functional area; information, personnel and physical security.

In order to implement an efficient and effective information security management framework, a role-based direct reporting structure in the case of the Institute is proposed. The advantage here is in handling exceptions which may need immediate attention and therefore information can be conveyed to the right person in minimum possible time. In view of the complexity related to IT at the Institute, the following key roles are proposed; ICT Steering Committee, ICT Manager, Deans, Heads of Department/ Section, Application Owners, Information Security Officer, IT Staff and, Users.

4.4 Roles and responsibilities

The ICT Steering Committee (ICTSC) will be responsible for information security management, to steer and oversee the activities pertaining to this Policy document and related Information Security Operations Manual. The Committee will monitor security violations and direct corrective action through the ICT Manager and Information Security Officer.

The details responsibilities for all the key parties are outlined in the Information Security operations Manual that must be used in conjunction with this policy document.

4.5 Monitoring, Review and Evaluation of Policy

Monitoring for compliance with the policy and procedures laid down in this document and the related information security operations manual will be done by the ICTSC together with independent reviews by both Internal and External Audit on a periodic basis.

It is the responsibility of the ICTSC to oversee the review and maintenance of this policy.

5.0 Benefits of policy

The information security policy is primarily concerned with people and how they go about using information assets as aided by the various information technology resources accessible at the Institute. The benefits of this policy to the Institute are outlined below;

a) To communicate to all people both internal and external that information is an asset, the property of the Institute and is to be protected from unauthorized access, modification, disclosure, and destruction,
b) To assure information resource users that the Institute provides a secure and trusted environment for the management of information used in delivering its programmes,
c) To clarify the different roles and responsibilities around information security expected of all action parties that interface with Institute business,
d) To set guidelines, best practices of use, and ensures proper compliance,
e) To strengthen the Institute's position in the event of any legal action that may arise.
f) To minimize risks of data leak or loss by ensuring that risks are identified and appropriate controls implemented and documented,

6.0 Due Diligence and Risk Management

In selecting a third party service provider the process followed must include due diligence of that third party. A risk assessment and a review of any proposed terms and conditions should be carried out to ensure that the Institute is not exposed to undue risk. This process may involve advice from but not limited to Institute members with expertise in a given field in question such as law, IT, information security, data protection and human resources. This process must also include the consideration of any information security policies or similar information available from the third party and whether they are acceptable to the Institute.

7.0 Policy violation

UMI provides qualified "Users" privileged access to its computing and networking resources. This privilege imposes certain responsibilities and obligations that are subject to the Institutes policies, regulations and National laws. All users must comply with these specific policies and guidelines governing their use, and act responsibly. This policy applies to all use whether initiated from a computer and/or network device located on or off campus.

"Violations of this policy are subject to sanctions prescribed in, but not limited to, the following policies: Staff Regulations Manual, Computer Misuse Act, 2011, The Uganda Public Service Standing orders, 2010 Edition."

References:

1. ISO/IEC 270001, 2005
2. National Information Security Policy, 2014
3. National IT Policy, 2012
4. The Computer Misuse Act, 2011
5. Human Resource Manual, 2011
6. Finance Policies and Procedures Manual, 2008