

MIZAN TEPE UNIVERSITY

TEPE CAMPUS

SCHOOL OF COMPUTING AND INFORMATICS

DEPARTMENT OF: INFORMATION SYSTEMS

ASSIGNMENT OF: INFORMATION SYSTEM SECURITY

COURSE CODE: INSY4081

GROUP MEMBERS NAME

ID No

- | | |
|-------------------------|-------------|
| 1. Amanuel Derese..... | NSR/0197/12 |
| 2. Behija Yussuf..... | NSR/0435/12 |
| 3. Zekarias Karie..... | NSR/2041/12 |
| 4. Misganaw Amanu..... | NSR/1404/12 |
| 5. Yohannis Biwota..... | NSR/2005/12 |

SUBMITTED TO: Ms. MARESHET K.

SUBMMATION DATE: JANUARY 26 2023

Information Protection Policy For

[MTU ICT CENTER]

Author :

Mizan Tepi University Information Systems 4th Year Students

1. Amanuel Derese.....NSR/0197/12
2. Behija Yussuf..... NSR/0435/12
3. Zekarias Karie..... NSR/2041/12
4. Misganaw Amanu..... NSR/1404/12
5. YohannisBiwota..... NSR/2005/12

Table of Contents

1. Introduction and general overview	5
1.1. Purpose	5
1.2. Scope	5
2. Policy	6
2.1. Data Protection	6
2.2. Human Resources security	7
2.3. Asset Management	7
2.4. Information Management	8
2.5. System Access Policy	8
2.6. User Authentication Standard	9
2.7. Acceptable Use Policy	10
2.8. Remote Access and Electronic Communication	12
2.9. System Changes and Configuration	12
2.10. Network and Communication Policy	13
2.11. Threat and Incident Management Policy	13
2.12. Workstation Security	14
2.13. Mobile Device Security	14
2.14. Business Application Management Policy	15
2.15. Backup	15
2.16. Encryption	15
2.17. Malware Protection	16
2.18. Physical Security Policy	16
2.19. Risk Management Policy	16

3. Responsibilities 17

 3.1. Chief Security Officer 17

 3.2. Security & Privacy Committee 17

 3.3. Managers 17

 3.4. All Staff 17

4. Compliance and Enforcement 18

 4.1. Definitions 18

5. References 19

1. Introduction and general overview

MTU ICT center will ensure the protection of all information assets within the custody of the Business.




High standards of confidentiality, integrity and availability of information will be maintained at all times.

1.1. Purpose

Information is a major asset that MTU ICT center has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Organization maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

The main objectives of this Policy are:

-  To define the general security policy for MTU ICT center Information Systems and the information stored, processed and transmitted by them, including outsourced services;
-  To define a uniform approach, ensuring a high degree of information systems security throughout MTU ICT center;
-  To define responsibilities with regards to information systems security;








This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

1.2. Scope

This Information Protection Policy applies to all the systems, people and business processes that make up the Business's information systems. This includes all Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the Organization who have access to Information Systems or information used for MTU ICT center purposes.

2. Policy

This policy is intended to help you make the best use of the computer resources at your disposal, while minimizing the cyber security risks. You should understand the following:

-  You are individually responsible for protecting the equipment, software and information in your hands. Security is everyone's responsibility.
-  Identify which data is non-public, which includes company confidential data, client data and personal data as further described below. If you do not know or are not sure, ask. Even though you cannot touch it, information is an asset, sometimes a priceless asset.
-  Protect equipment from loss & theft. Only store company data on encrypted devices.
-  Do not bypass established network and internet access connection rules.
-  Do not bypass or uninstall your virus checking or firewall software. ▪ Do not change or install any unauthorized software or browser 'plug-ins'.
-  Do not copy or store MTU ICT center data on external devices or unauthorized external locations (including cloud-based services which are not company approved services). Contact IT for the best solution for secured file transfer when this is required.
-  If you become aware of a potential or actual Security Incident, you must report the incident as soon as possible by sending an email to:

[Security@ MTUICTcenter.com](mailto:Security@MTUICTcenter.com)

The Policies and supporting Standards in this chapter must be read, understood, acknowledged and followed by all Staff. These set the ground rules under which MTU ICT center operates and safeguards its data and information systems to both reduce risk and minimize the effect of potential incidents.

2.1. Data Protection

MTU ICT CENTER takes the protection of personal data seriously and the security measures set forth in this policy are essential to ensure the data protection standards supporting the MTU ICT center Information Management Policy are met.

2.2. Human Resources security

Job definition and resourcing






Information security must be covered in the Group's Security Human Resources policy and standards. The HR policies should ensure, as a minimum, that security is adequately covered in job descriptions; that personnel are adequately screened, trained and that confidentiality agreements are signed by all new employees and contractors.

User training on Security Awareness

A training plan and training material must be in place to ensure that the right level of Security Awareness is created and maintained within the organization. Software developers and all other relevant personnel involved in the development of software for MTU ICT center are required to undertake secure development training on a periodic basis.



2.3. Asset Management

MTU ICT center uses a variety of information assets, ranging from laptops and mobile phones to servers. An inventory needs to constantly be maintained and must include the following details for all significant information assets belonging to, or used by the company:-

-  Asset name and characteristics
-  The information owner
-  The custodian of the information, and repository location (database etc.)
-  The sensitivity of the asset, due to regulations, laws, customer expectations or other requirements
-  Requirements for the asset regarding availability, uptime, business continuity, etc.

Hardware Management

At MTU ICT CENTER we take a hardware lifecycle approach to hardware management:

-  Only approved software configurations should be applied to new hardware;
-  End-of-Life hardware should be securely disposed





2.4. Information Management

Information Classification

The MTU ICT CENTER Information Security Policy focuses on the protection of the 3 components of information stored on MTU ICT CENTER systems: Confidentiality, Integrity & Availability, whilst ensuring Data Privacy. All MTU ICT CENTER information must be classified based on these 3 categories in order to allow implementation of the appropriate levels of protection in line with its criticality and to ensure that the controls applied to it are sufficient, and do not impair the company's business. Information classification requirements are detailed in the MTU ICT CENTER Information Management Policy.

Information Handling






Information, in electronic and physical formats, should be handled in accordance with the sensitivity, risk and classification of the information:

-  Ensure confidentiality agreements are in place before sharing data externally ▪ Check email addresses prior to sending any files.
-  Files should only be copied to removable storage when necessary and the storage should be encrypted.
-  Use restricted access storage areas whenever possible
-  Data disposal should be done in accordance with the Information Asset Handling and Protection Standard for End User.

2.5. System Access Policy

Access to information and systems in the possession of, or under the control of MTU ICT CENTER must be provided based on a least privilege, need to know basis. All MTU ICT CENTER computers must be protected by approved password-based access control systems.

Multi-factor authentication for remote access to corporate and production networks by employees, administrators, and third parties shall be implemented where available. The following rules must be maintained for managing user access rights:

-  **User registration:** approving and granting access rights to users on a need-to-know basis.
-  **Privilege management:** Clear hierarchies must be determined for each system, and each hierarchy must be formally approved. For example, for Oracle, there are 13 formally recognized authority levels, and any changes to that number or its composition must be formally approved by the Group's Controller.
-  **User management:** As above, each system must have clear procedures for approval and method of granting access to that system. Procedures must exist for each system for both joiners, movers and leavers, with audit trails.
-  User access rights are subject to periodic reviews.
-  Inactive user accounts must be configured to automatically disable after 90 days.

2.6. User Authentication Standard

- ✓ Users must be forced to change their passwords during the first log on, and at 60 - day intervals.
- ✓ Passwords shall not be displayed or transmitted in clear text and shall be suitably protected via approved cryptographic solutions.
- ✓ Passwords shall be stored in an encrypted format. A history of passwords shall be maintained to prevent the re-use of passwords
- ✓ A maximum of six successive login failures shall result in account lockout until an administrator unlocks it.
- ✓ Default accounts shall be disabled and/or default passwords associated with such accounts shall be changed

Password Selection

In order to make it harder to guess or steal your passwords

Please keep in mind the following

- ✓ Do not use dictionary words - All real words are easy to guess. Avoid using any words, words in foreign languages, swear words, slang, names, nicknames, etc.

- ✓ The names of family, friends and partners, anniversary dates, car registrations and telephone numbers are the first things tried when guessing your passwords.
- ✓ Instead try to use acronyms relevant to you only, mnemonics, random letters, etc., and insert non alphabetic characters in the middle of the word.
- ✓ Use a mixture of UPPER and lower case, numbers and special characters.
- ✓ When changing passwords, change more than just the number.
- ✓ However, choose something you can remember. It is no use having a strong password if you have it written on a Post-It Note on your desk! If you must have a reminder or hint, use something cryptic that only you can understand.
- ✓ Never tell anyone else your password or allow them to log in as you.
- ✓ Try to avoid letting other people watch you key-in your password. Choose something that is not easy to guess from watching
- ✓ Be aware of 'social engineering'. These are practices used to obtain personal information such as passwords, account numbers etc. (via fake web pages, e-mails, phone calls).

2.7. Acceptable Use Policy



Email Usage

E-mail is a business communication tool which all MTU ICT CENTER employees are requested to use in a responsible, effective and lawful manner.





Internet Usage

MTU ICT CENTER provides Internet access to all staff to assist them in carrying out their duties such as looking up details about suppliers, products, accessing governmental information and other work-related information. Occasional and limited personal use of the Internet is permitted if such use does not:






-  Interfere with work performance & productivity;

-  Include downloading or distribution of large files;
-  Have negative impact on the performance of MTU ICT CENTER' IT systems.

When using Internet access facilities, you should comply with the following guidelines:

-  Keep your personal use of Internet to a minimum.
-  Check that any information you use from the Internet is accurate, complete and current.
-  Respect the legal protections of data, software, copyright and licenses.
-  Do not download or transmit text or images which contain any software, material of obscene, threatening, racist or extreme political nature, or which incites violence, hatred or any illegal activity.

It is **STRICTLY FORBIDDEN** to upload Company non-public Information such as any of the following to external file transfer or storage sites, like Box, Drop box or Google Drive:

-  Source Code, object code, user documentation and all other software development details.
-  Company strategy and business plans
-  Intellectual Property, such as: Copyrights, Patents and Trade Secrets.
-  Information related to our clients' customers, including any details stored within MTU ICT CENTER software products, such as transaction or bank account details.
-  Any other company non-public information.

Portable Media

The use of portable media is not permitted. The intended purpose is to protect customer and company information from being transferred via unauthorized means. MTU ICT CENTER reserve the right to inspect and erase portable media that is used on our network.

2.8. Remote Access and Electronic Communication

Frequently users will be required to access the Group's Information systems from outside the office, for example travelling consultants and/or employees working in Sales / Business Solutions.

For remote access to the Corporate IT Infrastructure resources only the officially supported and approved facilities by the internal IT department are to be used (i.e., MTU ICT CENTER Secure Access Portal). The associated security policies must be applied.

Online Communication within MTU ICT CENTER offices to an external party may only use MTU ICT CENTER approved communication channels. Personal internet connections or connectivity devices (e.g., using personal data modems and Mobile Hotspot connections, remote access connections, personal VPNs etc.) **are strictly prohibited**. The detailed Electronic Communication Requirements are described in the dedicated policy named MTU ICT CENTER Network and Communications Policy.

2.9. System Changes and Configuration

All changes must be conducted in a controlled and approved way, in accordance with the IT Change Management Standard and IT System Configuration Standard.

System changes or re-configurations of standard IT components are not allowed. Only additions and/or changes of software components can be made by users on workstations based on customer project requirements. The following system changes are strictly prohibited

Installation of:

- ✓ Unauthorized connectivity devices (e.g., data modems);
- ✓ Any component suitable to gain unauthorized access to restricted areas; o Any other non-standard software or hardware component.
- ✓ Merging of two networks by physically integrating them on a network node;
- ✓ Disabling virus protection

2.10. Network and Communication Policy

Internet Usage

- ✓ External facing networks should be firewalled to an appropriate level
- ✓ WAN services should only be acquired through approved vendors
- ✓ Third-party users shall not connect their computing devices to the wired or wireless network of MTU ICT CENTER, unless authorized.

Wireless Networks

- ✓ Passwords for Guest wireless networks should be changed on a regular basis
- ✓ Only approved wireless access points should be used
- ✓ Wireless networks should always be encrypted

2.11. Threat and Incident Management Policy

Event Logging and Monitoring

Monitoring may consist of activities such as the review of:-

- ✓ Automated intrusion detection system logs
- ✓ Firewall logs
- ✓ User account logs
- ✓ Network scanning logs
- ✓ Application logs
- ✓ Help desk tickets
- ✓ Vulnerability Scanning
- ✓ Other log and error files

Any security issues discovered will be reported to the Information Security Department for investigation. Our detailed policy is set out in the Security Event Logging and Monitoring Standard.

User Monitoring

MTU ICT CENTER monitors many aspects of user behavior including but not limited to:

- ✓ Monitoring Internet access usage;
- ✓ Reviewing material downloaded or uploaded via the Internet;
- ✓ Reviewing e-mails sent or received by users, if there is a well-founded suspicion about a breach of provisions of this Policy or of applicable laws, or if there is a legal or regulatory requirement in this respect;
- ✓ Reviewing installed software on user's computers;
- ✓ Logins to and use of MTU ICT CENTER network as well as use of PCs.

2.12. Workstation Security

Workstations include laptops and desktops:

- ✓ All workstations should have corporate-approved antivirus software installed and enabled
- ✓ All workstations should have data loss protection software installed (where available)
- ✓ All laptops should be encrypted ▪ Only install software from trusted sources ▪ Do not allow unauthorized users to access your workstation
- ✓ Take appropriate steps to maintain the physical security of your workstation

2.13. Mobile Device Security

Every mobile device capable of accessing MTU ICT CENTER information shall be enrolled in the company MDM solution. access to a mobile device, the user should contact the local IT team and report the Security Incident to Information Security Team.

2.14. Business Application Management Policy

At MTU ICT CENTER we have a high dependency on software to conduct our day-to-day business:

- ✓ Applications should comply with the Privacy By Design principle.
- ✓ A Data Privacy Impact Assessment (DPIA) should be completed for major software changes that involve personally-identifiable information (PII).
- ✓ Security requirements for software should be documented as part of the development process
- ✓ Software changes should be subject to change control procedures
- ✓ Only authorized users are permitted to deploy software changes.

This policy only applies to software we develop for internal users e.g., Oracle E-Business, development of the MTU ICT CENTER Product Suite is outside the scope of this policy.

2.15. Backup

MTU ICT CENTER IT Service Continuity (DR) Policy provides a framework for ensuring that information in scope of this policy will not be lost during an incident affecting availability or integrity. Similarly, all media containing backups of MTU ICT CENTER data must be protected according to the data classification related to Data Confidentiality, Integrity & Availability, whilst ensuring data privacy. Both data classification and backup requirements must be determined by the asset owner and communicated to IT for implementation. Asset / data owners are responsible to inform Corporate IT in writing of the specific backup requirements for each asset or data set and of the required backup retention period in line with **IT Service Continuity (DR)**.

2.16. Encryption

Encryption is required to be used to protect Company non-public Information from being disclosed to unauthorized parties. All personnel are responsible for assessing the confidentiality level of data being sent or residing on the devices they use. If data is non-public, all MTU ICT CENTER employees are responsible to comply with the Encryption Standard.

2.17. Malware Protection

A process must be maintained to ensure that malicious software cannot enter the group's secure IT environment. This will include regular anti-malware updates, schedule malware scans and monitoring of events and incidents related to malware, detailed in MTU ICT CENTER Threat and Incident Management Policy.

2.18. Physical Security Policy

Access to every office, computer machine room, and other MTU ICT CENTER work areas containing sensitive information must be physically restricted to those people with a need to know. Every MTU ICT CENTER user must ensure that no important information asset shall be left on desks unattended, especially during non-work hours.

At MTU ICT CENTER our security is dependent on the physical security of our resources at purpose-built data centers and at on-premise computer rooms:

- ✓ Critical server rooms must be located in a place where the risk of natural disasters is within our risk appetite
- ✓ All entry points to IT facilities should be controlled with electronic access control mechanisms
- ✓ Appropriate environmental controls such as air conditioning and fire suppression systems should be in place
- ✓ There must at least be battery backup power onsite with sufficient duration to switch over to diesel power generation. If there is no diesel backup, then there should be 24 hours of battery power.
- ✓ Visitor access should be controlled
- ✓ Food and drink is not allowed in MTU ICT CENTER data centers.

2.19. Risk Management Policy

Our Information Security Risk Management framework is key to the way in which we identify and treat Information Security risks. Our approach is centrally managed but depends on regional and divisional support; therefore, Management should be familiar with the Risk Management Policy and of their role within the framework.

3. Responsibilities

Information Security is everyone's responsibility, although the ultimate responsibility resides with the Board of Directors and Executive Management. This responsibility cascades down through a series of designated roles.

3.1. Chief Security Officer

The Chief Security Officer is responsible for: ▪

- ✓ Information security management within MTU ICT CENTER, acting as a central point of contact on information security for both staff and external organizations;
- ✓ Managing and implementing this policy and related policies, standards and guidelines

3.2. Security & Privacy Committee

The Security & Privacy Committee is responsible for information risk within MTU ICT CENTER, advising the executive management on the effectiveness of management of security and privacy issues across the Group and advising on compliance with relevant legislation and regulations.

3.3. Managers

Managers shall be individually responsible for the security of their environments where information is processed or stored.

- ✓ Determining the level of access to be granted to specific individuals;
- ✓ Ensuring staff have appropriate training for the systems they use;
- ✓ Ensuring staff know how to access advice on information security matters.

3.4. All Staff

All staffs are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular, all staff should understand.

4. Compliance and Enforcement

All managers and supervisors are responsible for enforcing these policies. Employees who violate these policies are subject to discipline up to and including termination in accordance with the Practice's Sanction Policy.

4.1. Definitions

Information is a corporate asset. The Trust's Information Assets are important sources of administrative, clinical, evidential and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of the Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

For the purpose of this policy **Information Assets (IAs)** are 'identifiable and definable assets owned or contracted by the Trust which are valuable to the business of the organization'.

IAs will include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of data, and should not be seen as simply technical. Categories of IAs include:

- **Information:** Databases, system documents and procedures, archive media/data, paper records.
- **Software:** Application programs, systems, development tools and utilities.
- **Physical:** Infrastructure, equipment, furniture and accommodation used for data processing.
- **Services:** Computing and communications, heating, lighting, power, air-conditioning used for data processing.
- **People:** Their qualifications, skills and experience in the use of information systems.
- **Intangibles:** For example, public confidence in the organization's ability to ensure confidentiality, integrity and availability of personal data.

The **Information Asset Register** documents information about all information assets across the Trust, and includes information about each asset owner (Information Asset Owner) and administrators (Information Asset Administrators).

Information Risk Management – A methodical information security risk assessment process which ensures that the Trust identifies, implements and manages controls to monitor and reduce

the information security risks to the organization, its person identifiable information and its critical information assets.

An **information risk** is the chance of something happening to information which is held by the Trust or their contractors, which will have an impact upon the organizations' business objectives. Information risks are measured in terms of *consequence* and *likelihood*, in accordance with the Risk Management Procedure.

5. References

The policies and requirements included in this document are consistent with the Business Code of Conduct. Reference should also be made to the following:

- ✓ Acceptable Use Policy
- ✓ Information Security Governance Policy
- ✓ Information Risk Policy
- ✓ Human Resource Security Policy
- ✓ Information Management Policy
- ✓ IT Asset Management Policy
- ✓ Business Application Management Policy
- ✓ System Access Policy
- ✓ Systems Management Policy
- ✓ Network and Communication Policy
- ✓ Third Party Risk Management Policy
- ✓ Technical Security Management Policy
- ✓ Threat and Incident Management Policy
- ✓ Physical Security Policy
- ✓ Business Continuity Management Policy
- ✓ Security Assurance Policy