Kenya Water Institute
Training, Consultancy and Research in the Water Sector

KENYA WATER INSTITUTE (KEWI)

MIT DEPARTMENT

INFORMATION TECHNOLOGY & COMMUNICATION POLICY

EFFECTIVE 2018

Table of Contents

PREFACE 1

CHAPTER 1: INTRODUCTION 2

1.0 Introduction 2

1.1 Definitions 2

1.2 Policy Scope 2

1.3 Quality Policy Statement 2

1.4 Quality Objective Statement 2

1.5 Misuse of Computing Resources 3

1.6 Responsibilities of Users 5

1.7 Responsibilities of Director, Deputy Directors , Department Heads, and Supervisors 6

CHAPTER 2: ADMINISTRATIVE ACCESS TO LAN USER'S INFORMATION 7

2.0 Authorizations 7

2.1 Restrictions 7

CHAPTER 3: USER PRIVILEGE 8

2.0 Overview 8

3.1 Purpose 8

3.2 Local Computer Privileges 8

3.3 Network Privileges 8

CHAPTER 4: USE OF PASSWORD 10

3.0 Overview 10

4.1 Purpose 10

4.2 Scope 10

4.3 Password Protection 10

4.4 Password Requirements 11

4.5 Enforcement 12

4.6 Other Considerations 12

CHAPTER 5: ANTI-VIRUS 13

4.0 Overview 13

5.1 Purpose 13

5.2 Anti-Virus 13

5.3 Email Server 13

5.4 Email Malware Scanning 13

5.5 File Exchange 14
5.6 Network Exploit Protection 14
5.7 Other Malware 14
CHAPTER 6: EMAIL & INTERNET CONNECTION 15
5.0 Overview 15
6.1 Purpose 15
6.2 Physical Internet Connection 15
6.3 Use of the Internet 16
6.4 Internet Control and Logging System 16
6.5 No Sexually Explicit Sites. 17
6.6 Right to Monitor 17
6.7 Confidentiality. 17
CHAPTER 7: USE OF SOFTWARE 19
7.0 Overview 19
7.1. Software Purchasing 19
7.2 Workstations and Laptops 19
7.3 Licensing and Copyright 19
7.4 Hacking 20
7.5 Institute Supported Software 20
CHAPTER 8: APPLICATION IMPLEMENTATION 21
8.0 Overview 21
8.1 Purpose 21
8.2 Process 21
CHAPTER 9: ASSET CONTROL 22
9.0 Overview 22
9.1 Purpose 22
9.2 Assets Tracked 22
9.3 Asset Tracking Requirements 21
9.4 Asset Transfers 21
9.5 Asset Disposal 21
CHAPTER 10: BACKUP 22
10.0 Overview 22
10.1 Purpose 22

10.2 Scope 22
10.3 Definitions 22
10.4 Timing 22
10.5 Media Storage 22
10.10 Responsibility 22
10.11 Testing 22
10.12 Data Backed Up 22
10.13 Archives 23
10.14 Restoration 23
10.15 Media Storage Locations 23
CHAPTER 11: NETWORK & SERVER DOCUMENTATION 24
11.0 Overview 24
11.1 Purpose 24
11.2 Network Documentation 24
11.3 Server Documentation 25
11.4 Access 26
11.5 Change Notification 26
11.6 Documentation Review 27
11.7 Storage Locations 27
CHAPTER 12: IT EQUIPMENT PURCHASE AND FAILURE PREVENTION 28
12.0 Overview 28
12.1 Purpose 28
12.2 Scope 28
12.3 Critical Services 28
12.4 Equipment Requirements 28
12.5 Additional Requirements 28
CHAPTER 13: SERVER MONITORING 29
13.0 Overview 29
13.1 Purpose 29
13.2 Scope 29
13.3 Daily Checking 29
13.4 External Checks 29
CHAPTER 14 : USER TRAINING 30

14.0 Overview 30
14.1 Purpose 30
14.2 Training Categories 30
14.3 Requirements 31
CHAPTER 15: COMPUTER MAINTENANCE 32
CHAPTER 16: CONCLUSION 33
16.0 Enforcement / Disciplinary Action 33
14.4 Enforcement 33
3.4 Enforcement 33
APPENDIX 1: Computer Maintenance Request form 34
APPENDIX 1: Computer Maintenance Schedule 35

PREFACE

In order to protect our network, computers and the confidential data, KEWI has instituted this Information Systems and Network Policy.

This policy and the guidelines herein, set forth conditions for the use of information technology resources, including the Institute network equipment, access to outside networks through the local network, software, and digital media. We're protecting against not just the damages and liability created when unauthorized access occurs, but also against viruses and physical damage to our systems.

Therefore, all members of the Institute community must use all Institute computing and information resources and services in a manner that respects and maintains the public trust.

Endeavors have been made to keep the document simple to understand, to guide system administrators and users of these systems.

Employees are advised to contact the head of Information Technology whenever they are in difficulty and in need of advice, elaboration, definition or explanation for matters pertaining computer use.

This ICT Policy has been developed, in consultation with various experts in Information systems and with comparative references, to the ICT Board Laws and the General Kenyan Laws applicable to allow it become a legal document for the Management of systems in the Kenya Water Institute.

CHAPTER 1: INTRODUCTION

1.0 Introduction

This document sets forth standards which must be adhered to by all Users, contractors and any user granted access to any machine on the Local Area Network (LAN) at any time, whether physically present at the Institute or via remote access.

Failure to comply with the policies set forth in this document will result in disciplinary action, and may result in termination of employment.

1.1 Definitions

For the purposes of this document, a "User" is any user, employee, student, contractor, agent, temporary worker, vendor and any other person in a position to know or obtain information about computers or devices on the Local area Network (LAN).

The “Firewall” is a hardware or software device which protects the ports of computers on the LAN. For the purposes of this document, "Remote Access" shall mean access to the Local Area Network from any location outside the firewall by any method, including but not limited to Virtual Private Network (VPN), dial-in modem, frame-relay, cable-modem and any other method of accessing the LAN from outside the firewall.

1.2 Policy Scope

The Policy applies to any person granted authorization to access any computer or device on the Institute's LAN (an "Authorized User"). This includes but is not limited to contractors, temporary workers, vendors, sub-contractors and partners authorized to access any of the Institute's computers, locally or via Remote Access, for any reason, including email and Internet or intranet web browsing.

1.3 Quality Policy

“To provide comprehensive and trouble free IT environment in giving solutions to our highly valued users in all IT aspects and to be responsive technologically in information market.”

1.4 Objectives

- Ensure provision of adequate and reliable information systems
- Provide guidelines on the usage of ICT software, hardware and services
- Promote efficient utilization of ERP system for improved transaction processing and more accurate data entry and reporting.
- Ensure information security and enhance continuity of operations in the event of a disaster through regular backups.
- Continue to utilize cost-effective training methods to ensure the full use of existing information technology capabilities by institute students as well as by employees.
- Expand training opportunities that enable employees to update current technical knowledge and skills as the commercially available information technology tools that they rely upon are updated.

- Ensure that the IT management systems keep pace with future requirements and technology.

4.0 Scope

This ICT policy covers all IT facilities, hardware, software, and services provided by the Institute. These are:

a) Facilities

i. Computer labs
ii. Server room(s)
iii. ICT maintenance room
iv. All ICT facilities installed at KEWI

b) Services

Provision of guidance and expertise training on ICT
ICT support in software, hardware and any other computing infrastructure
Technical support to staff and students

c) Hardware

i. PCs
ii. Laptops
iii. Printers
iv. Scanners
v. Servers
vi. Network routers and switches
vii. Power backup equipment (e.g. Uninterruptable Power Backup - UPS)
viii. L.C.D Projectors
ix. Network Devices
x. Cameras (Digital and Camcorders)
xi. PDAs, Smartphones and other Mobile Computing Devices
xii. Diskettes/CDs/DVDs
xiii. Flash-disks/external hard-disks
xiv. PABXs, Telephone heads, fax and photocopiers
xv. All other ICT related hardware

d) Software

i. Network operating systems
ii. PC operating systems
iii. Application software
iv. Utility software
v. Custom made systems

KEWI Campuses

The policy all covers all KEWI Campuses. These will be supported from the KEWI Nairobi campus.

1.5 Misuse of Computing Resources

The following actions constitute misuse of the Institute's computer resources and are strictly prohibited for all Users:

1. Criminal and illegal acts. Institute computer resources are not to be used in support of or for illegal activities. Any such use will be reported and dealt with by the appropriate Institute authorities and/or law enforcement agencies. Criminal and illegal use may involve, but is not limited to, unauthorized access, intentional corruption or misuse of computer resources, theft, obscenity, and child pornography.

2. Failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of the Institute's computer resources.

3. Abuse of computer resources including, but not limited to, any act which endangers or damages specific computer software, hardware, program, network or the system as a whole, whether located on campus or elsewhere on the global Internet; creating or purposefully allowing a computer malfunction or interruption of operation; injection of a computer virus on to the computer system; sending a message with the intent to disrupt Institute operations or the operations of outside entities; print outs that tie up computer resources for an unreasonable time period to the detriment of other authorized users; computing tasks that consume an unreasonable amount of communications bandwidth either on or off campus to the detriment of other authorized users; and failure to adhere to time limitations which apply at particular computer facilities on campus.

4. Use of Institute computer resources for personal financial gain or a personal commercial purpose.

5. Failure to protect a password or account from unauthorized use.

6. Permitting someone to use another's computer account, or using someone else's computer account.

7. Unauthorized use, access, reading, or misuse of any electronic file, program, network, or the system.

8. Unauthorized use, access, duplication, disclosure, alteration, damage, misuse, or destruction of data contained on any electronic file, program, network, or Institute hardware or software.

9. Unauthorized duplication and distribution of commercial software and other copyrighted digital materials. All commercial software and many other digital materials are covered by a copyright of some form. The unauthorized duplication and distribution of software and other

copyrighted materials (including copyrighted music, graphics etc) is a violation of copyright law and this policy. Exceptions to this are specific authorization by the copyright holder or use under the fair use provisions of the copyright law.

10. Attempting to circumvent, assisting someone else or requesting that someone else circumvent any security measure or administrative access control that pertains to Institute computer resources.

11. Use of the Institute computer system in a manner that violates other Institute policies such as racial, ethnic, religious, sexual or other forms of harassment.

12. Use of the Institute's computer system for the transmission of commercial or personal advertisements, solicitations, promotions, or employees' transmission of political material that is prohibited

1.6 Responsibilities of Users

1. A user shall use the Institute computer resources responsibly, respecting the needs of other computer users.

2. A user is responsible for any usage of his or her computer account, computing resources or data entrusted to him or her. Users should maintain the secrecy of their password(s).

3. A user must report any misuse of computer resources or violations of this Policy to their department head or to the Chief Technology Officer.

4. A user must comply with all reasonable requests and instructions from the computer system operator/administrator.

5. When communicating with others via the Institute computer system, a user's communications should reflect high ethical standards, mutual respect and civility.

6. Users are responsible for obtaining and adhering to relevant network acceptable use policies including the Information Resources Security Policy and the Network Connections Policy.

1.7 Responsibilities of Director, Deputy Directors , Department Heads, and Supervisors

1. Ensure that employees within a department receive opportunities to attend training courses that help them to comply with this policy and other applicable Institute policies.

2. Promptly inform appropriate computer system administrator when employees have been terminated so that the terminated employee's access to Institute computer resources may be disabled.

3. Promptly report ongoing or serious problems regarding computer use to the system administrator.

CHAPTER 2: ADMINISTRATIVE ACCESS TO LAN USER'S INFORMATION

The following set of authorizations and restrictions is designed to enable LAN administrators to carry out their responsibilities while protecting the privacy of LAN users.

2.0 Authorizations

For purposes of system maintenance and management, LAN administrators are specifically authorized to acquire, store, and use the following types of information stored in computers attached to KEWI LAN:

LAN administrators are permitted unlimited access to a network user's computer when that user has given explicit consent for such access, as during installation, upgrade, trouble-shooting, and repair operations.

LAN administrators have read-only access to information about the current configuration of any user's networked computer, subject to the limitation that no user-input information is to be collected by the administrator. In practice, this authorization would allow the administrator to use software to identify the user's CPU, keyboard, and monitor types, amounts of free RAM and disk space, operating system and version, available ports, and similar useful configuration data such as that contained in generic configuration files.

LAN administrators have unlimited read and write access to one specified directory and its subdirectories on the networked computer and one specified individual-user-drive directory and its subdirectories on each attached server, subject to the limitations described later in this paragraph. For example the LAN administrator might select the network directory on the computer and the setups directory on the server's I: drive. However, these rights of special access shall be exercised only after users have been given one-time notice of the unusual privileges the administrator enjoys in these directories and their subdirectories.

LAN administrators are permitted to make back-up copies of all files stored on servers. These copies are to be used solely to protect against data loss.

LAN administrators are permitted to use software that identifies and directs specific file types on the network to specific network bandwidth areas. For example, .MP3 file types used for the sharing of recreational music shall have a limited operating bandwidth. This action is taken in the interest of protecting the maximum amount of network bandwidth for the academic purposes of the institute.

2.1 Restrictions

Except as noted above, it is the responsibility of KEWI that electronically stored information be treated as confidential. This confidential treatment refers not only to personal files but also to the content of keystrokes, files, printing queues, and other information-bearing materials sent on the network. Examining or disclosing the files and/or contents thereof is appropriate only if authorized by the owner of the information, approved in writing by the appropriate KEWI personnel

CHAPTER 3: USER PRIVILEGE

2.0 Overview

This defines the privileges various users on the organizational network are allowed to have, specifically defining what groups of users have privileges to install computer programs on their own or other systems. This defines the users who have access to and control of sensitive or regulated data.

This defines internet access to specific sites for some users or other ways they may or may not use their computer systems.

3.1 Purpose

It is designed to minimize risk to organizational resources and data by establishing the privileges of users of data and equipment on the network to the minimum allowable while still allowing users to perform job functions without undue inconvenience.

3.2 Local Computer Privileges

There are three main categories of users on a computer or network. These categories include:

1. Restricted user - Can operate the computer and save documents but can't save system settings.
2. Standard user (power user) - Can change many system settings and install programs that don't affect Windows system files.
3. Administrators - Have complete access to read and write any data on the system and add or remove any programs or change system settings. The majority of users on most common networks should be restricted users on their local computers. Only users with special training or a need for additional access should be allowed to change system settings and install programs that are not operating system programs. This is because many viruses and adware or spyware may be installed in a subtile manner by tricking the user or the installation may be completely transparent to the computer user. If the user does not have the ability to install programs or change settings to a more vulnerable setting, most of these potential security problems can be prevented.

Therefore only users that demonstrate a need and ability for power user or administrator access on local machines shall be permitted to have this level of access. Upon demonstration of a special need for additional access, the IT manager must approve the access before it can be made effective. Groups that may be allowed this type of access include:

1. Domain Administrators
2. Help Desk personnel
3. Application developers for testing purposes who have known computer training or skills.

3.3 Network Privileges

Most network users will have access to the following types of network resources.

1. Email - Most users will have full access to their own email. They will not be able to transfer ownership to someone else.

2. A personal network drive on a networked file server - This is a folder on a drive that only the primary user of this drive can read and write exclusive of domain administrators. The user will not be able to transfer ownership to someone else.
3. A shared group or organizational division's drive - This is a folder that members of specific groups or divisions in the organization may access. Access may be read or write and may vary by organizational requirements.
4. Access to databases - There may be additional databases that may be stored on a shared drive or on some other resource. Most databases will have a standard user level which gives users appropriate permissions to enter data and see report information. However only the database administrators will have full access to all resources on a database. Database administrators will only have full access to the database that they administer.

Groups that may be allowed additional access include:

1. Backup operator - Allowed to read data on the domain for the purpose of saving files to backup media. This group cannot write all data on the domain.
2. Account operator - Can manage and view information about user accounts on the domain.
3. Server operator - Has full privileges on servers including reading and writing of data, installing programs, and changing settings.
4. Domain administrator - Has full privileges on all computers in the domain including servers and workstations. Privileges include reading and writing data, installing programs, and changing settings.

CHAPTER 4: USE OF PASSWORD

3.0 Overview

All employees and personnel that have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

Employees or students must not use a password, access a file, or retrieve any stored communication, other than where authorized. All passwords are the property of KEWI. Employees or students may not use passwords on critical systems that have not been disclosed to the Information Technologist or other manager. Any compromised password should be reported to the account administrator. Student passwords are confidential and students are accountable for all usage under their password of the KEWI computer systems. Students should change their default password as soon as possible.

4.1 Purpose

It is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

4.2 Scope

This applies to any and all personnel who have any form of computer account requiring a password on the organizational network including but not limited to a domain account and e-mail account.

4.3 Password Protection

All Authorized Users must use strong passwords. Unacceptable passwords include but are by no means limited to,

- first or last names, or combinations thereof;
- names of an Authorized User's children or pets;
- words found in a dictionary, combinations of dictionary words with a sound alike digit (second2, etc);
- use of the words or variants on the word password, admin, update, access, login, computer, terminal, workstation, work, home, etc.
- Names of people or places as part of your password.
- Part of your login name in your password.

- ✓ Strong Passwords are a string of at least eight characters of upper and lower case letters and numbers.
- ✓ Authorized Users should change their password regularly.
- ✓ No User may leave a password written down in proximity to the computer or device which the password accesses.

- ✓ No User may ever provide their login or email password to anyone, including family members.

4.4 Password Requirements

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password which an attacker with the old password could guess. The following password requirements will be set by the IT security department:

1. Minimum Length - 8 characters recommended
2. Maximum Length - 14 characters
3. Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:
    1. Lowercase
    2. Uppercase
    3. Numbers
    4. Special characters such as !@#$%^&*(){}[]
4. Passwords are case sensitive and the user name or login ID is not case sensitive.
5. Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 24.
6. Maximum password age - 60 days
7. Minimum password age - 2 days
8. Store passwords using reversible encryption - This should not be done without special authorization by the IT department since it would reduce the security of the user's password.
9. Account lockout threshold - 4 failed login attempts
10. Reset account lockout after - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value as of the date of writing this article is 20 minutes. This means if there are three bad attempts in 20 minutes, the account would be locked.
11. Account lockout duration - Some experts recommend that the administrator reset the account lockout so they are aware of possible break in attempts on the network. However this will cause a great deal of additional help desk calls. Therefore depending on the situation, the account lockout should be between 30 minutes and 2 hours.
12. Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. they can press the CTRL-ALT-DEL keys and select "Lock Computer".
13. Rules that apply to passwords apply to passphrases which are used for public/private key authentication

4.5 Enforcement

Since password security is critical to the security of the organization and everyone, employees that do not adhere to this may be subject to disciplinary action up to and including dismissal.

4.6 Other Considerations

Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.

CHAPTER 5: ANTI-VIRUS

4.0 Overview

This defines anti-virus on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

5.1 Purpose

It is designed to protect the organizational resources against intrusion by viruses and other malware.

5.2 Anti-Virus

The organization will use an anti-virus product for anti-virus protection

1. The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.
2. The anti-virus library definitions shall be updated at least once per day.
3. Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

5.3 Email Server

The email server will have additional protection against malware since email with malware must be prevented from entering the network.

5.4 Email Malware Scanning

The scanner will scan all email as it enters the server and scan all email before it leaves the server. In addition, the scanner may scan all stored email once per week for viruses or malware.

When a virus is found or malware is found, the procedure shall be to delete the email and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. It would simply cause an additional help desk call by the notified person and most likely waste system administrator's time needlessly. Notifying the recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of help desk calls.

5.5 File Exchange

This specifies methods that are allowed to be used when files are sent into the network by members of the public or employees of the organization. It specifies:

1. All legitimate methods used including:
    1. FTP transfer to a FTP server.
    2. File transfer to a Web server with a legitimate file upload program.
    3. Any other method.
2. The method and type of software to be used to scan the files for hosile content before they are completely transferred into the network. It will also specify the update frequency for the scanning software.
3. The point in time when the files will be scanned.

5.6 Network Exploit Protection

This will specify that all systems be protected by a firewall any time they are connected to the internet. It would specify that systems on the organizational network be connected to a part of the network that is protected from the internet or untrusted network by an approved firewall system. It will also specify that computers operating outside the organizational network to have a local firewall software program operational at all times when these computers are connected to the internet. It should specify one or more acceptable software firewall products. This may refer to the mobile computer which may require users of mobile computers to have their computers checked for malware before connecting to the main network.

5.7 Other Malware

This should cover any other possible malware including adware and spyware. It may specify methods to prevent and remove this type of malware. It may specify acceptable prevention and removal software. If the anti-virus product is a product that also handles other types of malware such as adware or spyware, it should be stated here.

CHAPTER 6: EMAIL & INTERNET CONNECTION

5.0 Overview

This has components of a user compliance policy and an internal IT policy.

- The user compliance section specifies how users are allowed to connect to the internet and provides for IT department approval of all connections to the internet or other private network. It requires all connections such as connections by modems or wireless media to a private network or the internet be approved by the IT department and what is typically required for approval such as the operation of a firewall to protect the connection.

- This internet connection requires users to use the internet for business only and requires users to avoid going to malicious web sites which could compromise security. It informs the users that their internet activity may be logged and monitored and defines whether user activity on the network will be logged and to what extent. It specifies what system will be used to prevent unauthorized viewing of sites and what system will log internet usage activity. Defines whether a proxy server will be used for user internet access. It defines how the network will be protected to prevent users from going to malicious web sites.

Electronic mail, Internet access, and other electronic media and equipment are business tools that are provided by KEWI to employees and students to facilitate timely and efficient conduct of business. This addresses access, use and disclosure of electronic mail and Internet messages and material created, sent or received by KEWI employees and students using the institute 's systems. KEWI intends to honor the policies set forth below, but reserves the right to change them at any time, without notice as may be appropriate.

Limited personal use of the electronic mail and Internet/LAN systems is permitted, but should not be excessive or interfere with normal operations of the institute . KEWI reserves the right to restrict access to non-essential services.

6.1 Purpose

This is designed to protect the organizational resources against intrusion by malware that may be brought into the network by users as they use the internet. It is also designed to prevent unauthorized and unprotected connections to the internet which may allow a host of unsafe content to enter the organizational network and compromise data integrity and system security across the entire network.

6.2 Physical Internet Connection

All physical internet connections or connections to other private networks shall be authorized and approved by the IT department. Most users will access the internet through the connection provided for their office by the IT department. Any additional connections must be approved by the IT department. These additional connections include but are not limited to:

1. Modem connection from a computer or communication device which may allow a connection to the network.
2. Any multipurpose printing and FAX machines which have both a phone and network connection must be examined and approved for use by the IT department.
3. Wireless access points or devices with wireless capability are not allowed unless approved by the IT department. If any computers or other devices have wireless capability, the wireless capability must be turned off before connecting to the network unless it is approved for wireless operation by the IT department when connected to the network.

Any additional internet connections not provided by the IT department must be reviewed and approved by the head of management services unit. Typically any additional connections from the organizational network to the internet or other private network will require.

1. An IT department approved firewall operating at all times and properly configured.
2. Some communications through the connection may require encryption subject to a review of data to be transmitted by the IT department.

6.3 Use of the Internet

1. All employee use of the internet shall be for business purposes only.
2. Employee use of the internet may be monitored and logged including all sites visited, the duration of the visits, amount of data downloaded, and types of data downloaded. The time of recorded activity may also be logged.
3. Employees are urged to use caution when visiting unknown internet sites and through user training set and keep their browser configured to IT approved standards in order to protect against infections of malware. Employees will be trained in the latest IT approved standards to protect against malware when appropriate.

6.4 Internet Control and Logging System

The electronic mail and Internet/LAN systems and hardware are institute property. Additionally, all documents, messages and attachments composed, sent, received or stored on the electronic mail or Internet/LAN storage systems are and remain the property of KEWI.

A system will be required to operate on the network with the following capabilities:

1. The ability to prevent users from visiting inappropriate, pornographic, or dangerous web sites. It will have its database of categorized websites updated regularly.
2. The ability to log user internet activity including:
    1. Time of the internet activity.
    2. Duration of the activity.
    3. The website visited.
    4. Data and type of data downloaded
    5. Whether the system will cache web pages to increase the internet connection speed. This requires a proxy server.

3. The system (will / will not) require a login ID or it will use the current network login to identify users.

The system used to prevent users from visiting inappropriate, pornographic, or dangerous web sites. This same system will not require an additional login ID and will use Active Directory to identify internet users. The system shall be able to log the time of internet activity, duration of the activity, the website visited, any data downloaded and the type of data downloaded. The system will cache web pages.

6.5 No Sexually Explicit Sites.

KEWI's Internet system must not be used to visit sexually explicit or otherwise offensive or inappropriate Web sites, or to send, display, download or print offensive material, pornographic or sexually explicit pictures or any other materials which would be found offensive by most reasonable people. Content filters which are designed to disrupt access to these materials must not be bypassed or altered without prior approval of the Systems Administrator.

The electronic mail and Internet/LAN systems may not be used to solicit or proselytize for outside or personal commercial ventures, religious or political causes, outside organizations, or other solicitations that are not job-related. KEWI may at a time of its choosing provide access to a public electronic bulletin board system which will facilitate voluntary participation in non-business related messages and other transactions.

6.6 Right to Monitor.

KEWI reserves and intends to exercise the right to review, audit, intercept, access and/or disclose any and all traffic in the system, including messages or material, including attachments created, received or sent, web sites visited and/or files downloaded over the institute 's electronic mail or Internet/LAN systems. Authorized representatives of the institute may monitor the use of its systems in its sole discretion, at any time, with or without notice to any student and may by-pass any password. Such monitoring is capable of tracking and recording e-mail messages sent and received as well as web sites visited by employees and students.

6.7 Confidentiality.

The confidentiality of any message or material should not be assumed. Even when a message or material is erased, it may still be possible to retrieve and read that message or material. Further, the use of passwords for security does not guarantee confidentiality. Messages read in HTML may identify the reader to the sender. Notwithstanding, KEWI's right to retrieve and read any electronic mail or Internet messages or material, such messages or material should be treated as confidential by other employees or students and accessed only by the intended recipient. Employees and students are responsible for maintaining the confidentiality

of material on the systems. Without prior authorization from the Information Technologist, employees or students are not permitted to retrieve or read e-mail messages that are not sent to them. The contents of electronic mail or Internet messages or material may, however, be disclosed to others with prior authorization from the Information Technologist.

6.8 Internet Site/Identification Originator.

Employees and students should be aware that Internet sites accessed from KEWI's computer network may identify the institute as the originator of each visit. If employees participate in "chat sessions" or post messages on the Internet, they may be regarded as representing the institute. Thus, all communications must be professional, appropriate to KEWI, and not adversely reflect upon its reputation.

CHAPTER 7: USE OF SOFTWARE

7.0 Overview

This restricts the software that may be installed on Institute computers in order to ensure the appropriate use of ICT equipment, protect the integrity of the local network, and maximize available resources.

This place limitations on the copying and transfer of copyrighted materials. Respect for intellectual labour and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledge, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments.

Violation of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may lead to disciplinary action under the Institute disciplinary and dismissal procedure.

7.1. Software Purchasing

All software must be purchased through ICT Support with the written agreement of the System Administrator. This includes any external purchases such as Web Hosting / sites, online tools, etc.

7.2 Workstations and Laptops

Software shall not be installed, loaded or run on any ICT equipment that has not been approved for installation by the System Administrator. Staff who wish to have software installed on their office computers other than the standard applications listed below (Appendix 1) must submit a request in writing to the System Administrator.

As part of the regular inventory process Information Technology Services staff will perform a periodic audit of software installed on Institute machines in order to assure compliance with all relevant policies. Unauthorized software will be subject to immediate removal, even if stored in the Users My Documents.

7.3 Licensing and Copyright

All users of computer facilities are expected to understand and comply with the copyright laws as they apply to computer software and its documentation, and to refrain from creating or using illegal copies of software on Institute's computing equipment.

KEWI's Software use provides additionally that:

- Only properly licensed software shall be installed on computers.
- All software and data files stored on Institute-owned computer equipment must be consistent with the Institute's Acceptable Use and must not introduce technical problems that interfere with the proper functioning of other programs.

Additionally, all installed software must fall into one of the following categories:

• It is in the public domain.
• It is covered by a licensing agreement with the software author, authors, vendor or developer, whichever is applicable.
• It has been donated to the college by the author, authors, vendor or developer and a written record of the contribution is on file in the office of the System Administrator.
• It has been purchased by the Institute and a record of that purchase is on file with the System Administrator.
• It has been purchased by the user, approved for installation by ICT Support, and a record of a that purchase exists and can be produced by the user upon demand.
• It is a demonstration version of the software being reviewed by the user in order to reach a decision about possible future purchase or request for contribution or licensing.

When software is to be installed on a disk sharing system or computer network, efforts will be made to secure this software from being illegally copied.
Archival or backup copies of application or data files may be made only as specified by applicable license agreements.
The legal or insurance protection of KEWI will not extend to College employees who violate copyright laws or specific conditions of applicable software.

7.4 Hacking

The Institute has a 'Zero Tolerance' when it comes to the making, supplying or possession of any software that can be used for unauthorised access into computer networks and other ICT systems.

Any breach of this will lead to disciplinary action being taken against those staff or students involved.

7.5 Institute Supported Software

A list of Software supported by the Institute is available on request from the System Administrator.
Only legitimately acquired software may be used and only in accordance with all applicable licence conditions.
A software register (to include software name, serial number of product, date of purchase and the location of software) should be established and maintained to enable verification of software compliance.

CHAPTER 8: APPLICATION IMPLEMENTATION

8.0 Overview

This is to be used to assess the security impact of new applications. When new applications are developed to provide new functionality to customers or internal groups, the impact of the new functionality must be assessed in order to keep the network stable. Starting with a data assessment process will help this process flow smoothly.

8.1 Purpose

It is designed to protect the organizational resources on the network by defining requirements for new applications in the organization. This requires a security assessment including an assessment of data security levels, media the data will travel over, a risk evaluation, and determination of system requirements which will mitigate the most serious part of additional security risks.

8.2 Process

Customers shall work together with application developers and computer security experts to assess data requirements for any new applications. Customers shall specify their requirements for the applications and application developers will work with the customer to identify and categorize data according to the Application Development Security Assessment Process.

Once the data and application requirements are established, computer security personnel can then evaluate risk and determine methods, processes, equipment, and procedures to mitigate known risks. The computer security personnel, customers, and application developers will work together to provide required and reasonable access capability to systems and data both during development and final project implementation while providing the best computer security possible for a reasonable cost. Under no circumstances should the overall security of the network be seriously compromised for the benefit of any project.

The data assessment, risk evaluation, and system requirements should be done early in the project life cycle since without this information, the overall cost of the project cannot be accurately assessed.

CHAPTER 9: ASSET CONTROL

9.0 Overview

All employees and personnel that have access to organizational computer systems must adhere to the IT asset control in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control will not only enable organizational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This also covers disposal of assets.

IT assets should not be confused with nor tracked with other organizational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A special IT asset tracking will enable the organization to take measures to protect data and networking resources.

This will define what must be done when a piece of property is moved from one building to another or one location to another. This will provide for a asset tracking database to be updated so the location of all computer equipment is known. This will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the network. This also covers the possibility that data on a computer being moved between secure facilities may be sensitive and must be encrypted during the move.

9.1 Purpose

It is designed to protect the organizational resources on the network by establishing a procedure for asset control. It will help prevent the loss of data or organizational assets and will reduce risk of losing data due to poor planning.

9.2 Assets Tracked

This section defines what IT assets should be tracked and to what extent they should be tracked.

IT Asset Types

This section categorizes the types of assets subject to tracking.

1. Desktop workstations
2. Laptop mobile computers
3. Printers, Copiers, FAX machines, multifunction machines
4. Handheld devices
5. Scanners
6. Servers
7. Firewalls
8. Routers
9. Switches

9.3 Asset Tracking Requirements

1. All assets must have a Serial Number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified.
2. An asset tracking database shall be created to track assets. It will include all information on the Asset Transfer Checklist table and the date of the asset change.
3. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

9.4 Asset Transfers

This applies to any asset transfers including the following:

1. Asset purchase
2. Asset relocation
3. Change of asset trustee including when an employee leaves or is replaced.
4. Asset disposal

9.5 Asset Disposal

Asset disposal is a special case since the asset must have any sensitive data removed prior to disposal. Any data storage devices. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

1. None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
2. Low (Sensitive) - Erase the data using any means such as reformatting or degaussing.
3. Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
4. High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques. Approved technologies are to specified in a Media Data Removal Procedure document by asset type including:
    1. Floppy disk
    2. Memory stick
    3. CD ROM disk
    4. Storage tape
    5. Hard drive.
    6. RAM memory
    7. ROM memory or ROM memory devices.

CHAPTER 10: BACKUP

10.0 Overview

This defines the backup for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the ERP server.

10.1 Purpose

It is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

10.2 Scope

This applies to all equipment and data owned and operated by the organization.

10.3 Definitions

1. Backup - The saving of files onto offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
2. Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
3. Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

10.4 Timing

Full backups are performed 11.pm daily

10.5 Media Storage

There shall be separate sets of storage media

10.10 Responsibility

The IT Systems Administrator shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

10.11 Testing

The ability to restore data from backups shall be tested at least once per month.

10.12 Data Backed Up

Data to be backed up include the following information:

1. User data stored on the hard drive.
2. System state data
3. The registry

Systems to be backed up include but are not limited to:

1. File server

2. Mail server
3. Production database server
4. Domain controllers
5. Test database server

10.13 Archives

Archives are made at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

10.14 Restoration

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

10.15 Media Storage Locations

Offline storage media used for daily backup shall be stored in a fireproof safe.

CHAPTER 11: NETWORK & SERVER DOCUMENTATION

11.0 Overview

This defines the level of network documentation required such as documentation of which switch ports connect to what rooms and computers. It defines who will have access to read network documentation and who will have access to change it. It also defines who will be notified when changes are made to the network.

11.1 Purpose

It is designed to provide for network stability by ensuring that network documentation is complete and current. This should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

11.2 Network Documentation

The network structure and configuration shall be documented and provide the following information:

1. IP addresses of all devices on the network with static IP addresses.
2. Server documentation on all servers as outlined in the "Server Documentation" document.
3. Network drawings showing:
    1. The locations and IP addresses of all hubs, switches, routers, and firewalls on the network.
    2. The various security zones on the network and devices that control access between them.
    3. The locations of every network drop and the associated switch and port on the switch supplying that connection.
    4. The interrelationship between all network devices showing lines running between the network devices.
    5. All subnets on the network and their relationships including the range of IP addresses on all subnets and netmask information.
    6. All wide area network (WAN) or metropolitan area network (MAN) information including network devices connecting them and IP addresses of connecting devices.
4. Configuration information on all network devices including:
    1. Switches
    2. Routers
    3. Firewalls
5. Configuration shall include but not be limited to:
    1. IP Address
    2. Netmask

3. Default gateway
4. DNS server IP addresses for primary and secondary DNS servers.
5. Any relevant WINS server information.

6. Network connection information including:
    1. Type of connection to the internet or other WAN/MAN including T1,T3, frame relay.
    2. Provider of internet/WAN/MAN connection and contact information for sales and support.
    3. Configuration information including netmask, network ID, and gateway.
    4. Physical location of where the cabling enters the building and circuit number.
7. DHCP server settings showing:
    1. Range of IP addresses assigned by all DHCP servers on all subnets.
    2. Subnet mask, default gateway, DNS server settings, WINS server settings assigned by all DHCP servers on all subnets.
    3. Lease duration time.

11.3 Server Documentation

For every server on a secure network, there are a list of items that must be documented and reviewed on a regular basis to keep the institute network secure. This list of information about every server should be created as servers are added to the network and updated regularly.

1. Server name
2. Server location
3. The function or purpose of the server.
4. Hardware components of the system including the make and model of each part of the system.
5. List of software running on the server including operating system, programs, and services running on the server.
6. Configuration information about how the server is configured including:
    1. Event logging settings
    2. A comprehensive list of services that are running.
    3. Configuration of any security lockdown tool or setting
    4. Account settings
    5. Configuration and settings of software running on the server.
7. Types of data stored on the server.
8. The owners of the data stored on the server.
9. The sensitivity of data stored on the server.
10. Data on the server that should be backed up along with its location.
11. Users or groups with access to data stored on the server.
12. Administrators on the server with a list of rights of each administrator.
13. The authentication process and protocols used for authentication for users of data on the server.

14. The authentication process and protocols used for authentication for administrators on the server.
15. Data encryption requirements.
16. Authentication encryption requirements.
17. List of users accessing data from remote locations and type of media they access data through such as internet or private network.
18. List of administrators administrating the server from remote locations and type of media they access the server through such as internet or private network.
19. Intrusion detection and prevention method used on the server.
20. Latest patch to operating system and each service running.
21. Groups or individuals with physical access to the area the server is in and the type of access, such as key or card access.
22. Emergency recovery disk and date of last update.
23. Disaster recovery plan and location of backup data.

Mail Server Documentation

1. Account size limit where the person receives warnings about mailbox size
2. Account size limit where the person cannot send mail anymore.
3. Account size limit where the person cannot receive mail anymore.

11.4 Access

The IT networking and some enterprise security staff shall have full access to all network documentation. The IT networking staff shall have the ability to read and modify network documentation. Designated enterprise security staff shall have access to read and change network documentation but those not designated with change access cannot change it. Help desk staff shall have read access to network documentation.

11.5 Change Notification

The help desk staff, server administration staff, application developer staff, and IT management shall be notified when network changes are made including.

1. Reboot of a network device including switches, routers, and firewalls.
2. Changes of rules or configuration of a network device including switches, routers, and firewalls.
3. Upgrades to any software on any network device.
4. Additions of any software on any network device.
5. Changes to any servers which perform significant network functions whether configuration or upgrade changes are made. These servers include:
    1. DHCP
    2. DNS
    3. Domain controllers
    4. WINS

    Notification shall be through email to designated groups of people.

11.6 Documentation Review

The network or IT manager shall ensure that network documentation is kept current by performing a monthly review of documentation or designating a staff member to perform a review. The remedy or help desk requests within the last month should be reviewed to help determine whether any network changes were made. Also any current or completed projects affecting network settings should be reviewed to determine whether there were any network changes made to support the project.

11.7 Storage Locations

Network documentation shall be kept either in written form or electronic form in a minimum of two places. It should be kept in two facilities at least two miles apart so that if one facility is destroyed, information from the other facility may be used to help construct the IT infrastructure. Information in both facilities should be updated monthly at the time of the documentation review.

CHAPTER 12: IT EQUIPMENT PURCHASE AND FAILURE PREVENTION

12.0 Overview

This provides a guideline for the purchase of IT equipment when the equipment supports organizational identified critical services. This will name critical services and provide a guideline for purchasing technologies that are failure tolerant.

12.1 Purpose

It is to ensure that critical services are not interrupted by a single common failure. It provides standard guidelines to allow IT equipment purchased for essential services to have reliability built into the equipment. This is to prevent service outage for critical services.

12.2 Scope

This covers any computers providing critical services to the organization.

12.3 Critical Services

Critical services which are required for normal operation of the organization include:

1. File sharing service on a file sharing server.
2. Web services to the internet
3. Email services
4. Database services for internal users and critical external applications.
5. Critical external application servers.
6. Domain controller servers
7. Firewall to connect these services to the internet.

Any servers or equipment that supports these services should adhere to this including connection equipment from the internet to these services.

12.4 Equipment Requirements

All critical services are required to utilize redundant technologies including:

1. Dual power supplies on all servers providing critical services.
2. RAID disk arrays to prevent one disk failure from interrupting services
3. Uninterruptable power supplies that can provide power for a minimum of 1 hour to servers operating critical services in the event of a power outage.

12.5 Additional Requirements

For services that are critical for income or operations that cannot be interrupted the following technologies are also recommended:

1. A backup generator to ensure that long term power outages cannot interrupt service.
2. More than one server for the same service where the servers use clustering or load balancing technology.

CHAPTER 13: SERVER MONITORING

13.0 Overview

This defines the monitoring of servers in the organization for both security and performance issues.

13.1 Purpose

It is designed both to protect the organization against loss of service by providing minimum requirements for monitoring servers. It provides for monitoring servers for file space and performance issues to prevent system failure or loss of service.

13.2 Scope

This applies to all production servers and infrastructure support servers including but not limited to the following types of servers:

1. File servers
2. Database servers
3. Mail servers
4. Web servers
5. Application servers
6. Domain controllers
7. FTP servers
8. DNS servers

13.3 Daily Checking

All servers shall be checked manually on a daily basis the following items shall be checked and recorded:

1. The amount of free space on each drive shall be recorded in a server log.
2. The system log shall be checked and any major errors shall be checked and recorded in the server log.
3. Services shall be checked to determine whether any services have failed.
4. The status of backup of files or system information for the server shall be checked daily.

13.4 External Checks

Essential servers shall be checked using either a separate computer from the ones being monitored or a server monitoring service. The external monitoring service shall have the ability to notify multiple IP personnel when a service is found to have failed. Servers to be monitored externally include:

1. The mail server
2. The web server
3. External DNS servers
4. Externally used application servers.
5. Database or file servers supporting externally used application servers or web servers.

CHAPTER 14 : USER TRAINING

14.0 Overview

This defines the minimum training for users on the network to make them aware of basic computer threats to protect both themselves and the network. This especially applies to employees with access to sensitive or regulated data.

The training of computer users will benefit the organization in both increased productivity but also fewer security incidents.

Given the current state of computer security and the fact that many attacks are directly against the user's web browser or through e-mail, user training is becoming an ever more important part of computer security. User's must be wise to the methods of attack in order to protect themselves in many instances. User training does not need to be extremely technical but should ensure that the user retains basic computer knowledge along with some knowledge about specific computer attacks that they may experience.

14.1 Purpose

It is designed to protect the organizational resources on the network and increase employee efficiency by establishing user training. When users are trained about computer use and security threats, they work more efficiently and are better able to protect organizational resources from unauthorized intrusion or data compromise. This will help prevent the loss of data and organizational assets.

14.2 Training Categories

Training categories will include but not be limited to the following areas:

- Basics:
    1. What files are
    2. How to set view for details and show extensions for known file types
    3. Why not seeing file extensions is a security hazard to you
    4. File storage size - how to determine
    5. Mail attachments
    6. Where to store files
        - How to use your network drive
        - What your network drive is and what it means to you
    7. How to copy files
    8. Ways to increase efficiency on the computer such as keyboard shortcuts
- Ways to get malware:
    1. Through email
    2. Through browser
    3. By connecting
    4. By installing unapproved programs
- Email viruses:
    1. How they spread

    2. Spoofing sender
    3. Dangerous attachments
- Email SPAM
    1. Protect your email address
    2. Filtering spam
- Hoaxes:
    1. Phishing
    2. Fraud methods
- Email use
    1. How to set up email for remote users or with your ISP with POP3
    2. How to set up out of office reply
    3. How to set mail filtering rules
    4. How to use, import, and export personal folders
    5. What an undeliverable response to an email message means
- Use of web browser
    1. Safe browser?
    2. Avoid adware and spyware - ignore ads that may compromise your computer or get you to install an illicit program
    3. How to change browser settings for better security
    4. Products to prevent malware.
- Passwords
    1. Why protect my password?
    2. Why do I need to change my password every 30 days
    3. How to change your password
    4. How to choose strong passwords that you can remember
    5. If I log in on a website can someone see my password?
- Other
    1. Reasons for firewall -- worms and others
    2. Why worry about malware?
    3. What is a vulnerability?
    4. Why not run all services?
    5. Social engineering

14.3 Requirements

All organizational staff shall make measurable and continuous progress in the training areas. Each employee manager shall be responsible for ensuring that employees under their supervision make progress in the required training areas.

CHAPTER 15: COMPUTER MAINTENANCE

Computers should work perfectly all the time. Set them up once, and they just work, right? The truth is that your computer network is a collection of complex machines and software, communicating simultaneously, performing trillions of calculations, using hundreds of parts and wires, and under constant assault by the processing needs of the applications, unwanted viruses and spyware and their own users. Here are ten reasons every small business needs regular and proactive server and workstation maintenance:

1. Microsoft critical security updates need to be applied at least once a month
2. Firewall, virus and spyware protection needs regular review and management
3. Daily use of servers and workstations by office staff can create random network issues
4. Management of backup status, data selected and data testing is critical to data recovery
5. Proactive server and workstation standardization minimizes problems
6. Management of hard drive resources prevents storage issues & server crashes
7. Analysis of server event logs can identify issues before they create network problems
8. Regular optimization of server(s) and workstations to increase speed and efficiency
9. Proactive maintenance provides real peace of mind that someone is regularly caring for your network
10. Predictable monthly budget and support minimizes financial and technical surprises

Because of these and other factors, computers require regular computer service maintenance to keep the big problems away and maintain optimal performance.

The forms in the appendices are designed to assist the system administrator maintain the computer systems in their day to day operations.

CHAPTER 16: CONCLUSION

16.0 Enforcement / Disciplinary Action

Since improper use of computers can bring in hostile software which may destroy the integrity of network resources and systems and the prevention of these events is critical to the security of the organization and all individuals, employees that do not adhere to this may be subject to disciplinary action up to and including dismissal and/or pursuit of legal action.

Since data security and integrity along with resource protection is critical to the operation of the organization, employees that do not adhere to this may be subject to disciplinary action up to and including dismissal.

14.4 Enforcement

Since security is very important to the organization, auditing shall be used as a mechanism to be sure the training is being followed. Auditors may test employees at random about their knowledge in the areas listed above

3.4 Enforcement

Example

Server operators will have full access on some servers but not others.

Help desk personnel may have full access on some local computers but not in all groups in our organization.

APPENDIX 1: Computer Maintenance Request form

KEWI/ISO/ICT/001

KENYA WATER INSTITUTE

COMPUTER SYSTEMS MAINTENANCE REQUEST (To be used to report any faults with computer systems, internet and network or software related problems)	***REQUESTED BY:***_____ Phone No/Email:_____	DATE:_____
	LOCATION OF COMPUTER: OFFICE _____OTHER:_____	

AREAS OF REQUEST (Check all that apply)

☐	Computer not powering on	☐	No Internet connection	☐	Windows has crashed (Blue screen)
☐	Mouse faulty/ Moves Too Quickly (Slowly)	☐	No Network/Network cable seems	☐	Virus infection/No antivirus software
☐	Monitor not displaying		unplugged	☐	Data/File lost
☐	Keyboard not working	☐	Drive/Flash disk not being detected	☐	Windows Out Of Date
☐	No sound from the speaker	☐	Unable to send/receive Emails /	☐	Cannot log to ERP/GIS/Network Folder
☐	Printer Problems		Email setup Error	☐	ERP Error Message
☐	Computer too slow	☐	UPS power issue/noisy etc	☐	Other_____

FOR OFFICIAL USE ONLY - DETAILS OF PROBLEM

☐ KEYBOARD	☐ HARD DRIVE	☐ EMAIL	Other Hardware:_____
☐ MOUSE	☐ PRINTER	☐ NETWORK/INTERNET	
☐ CABLES/POWER	☐ MONITOR	☐ OFFICE / OTHER SOFTWARE	Routine maintenance (e.g. Antivirus, Backup, Defragmentation, Restore etc):
☐ MEMORY	☐ CD/DVD DRIVE	☐ ERP	_____

TYPE OF REQUEST ☐REPAIR ☐UPGRADE ☐OTHER(Specify)_____

ACTION TAKEN _____

_____

Signature (IT/AIT)_____ ***Date***_____

User Comment_____

APPENDIX 1: Computer Maintenance Schedule

	Computer Maintenance Schedule 2018											
Task	**January**	**February**	**March**	**April**	**May**	**June**	**July**	**August**	**September**	**October**	**November**	**December**
Download Virus Updates	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily
Incremental Backup	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily
Run Cleanup	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily
File Management	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily
Perform Full Virus Scan	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily
Run Spyboot and Adware	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily	Daily
Organize All Programs Menu	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly
Perform Full Backup	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly
Run Start Inspector	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly	Weekly
Check Windows Updates	X	X	X	X	X	X	X	X	X	X	X	X
Uninstall Unsued Programs	X	X	X	X	X	X	X	X	X	X	X	X
Clean Registry	X	X	X	X	X	X	X	X	X	X	X	X
Clean up Hard Disk	X	X	X	X	X	X	X	X	X	X	X	X
Update Drivers/Programs	X			X			X			X		
Clean Keyboard/Mouse	X			X			X			X		
Clean Monitor	X			X			X			X		
Defrag Hard Disk	X	X	X	X	X	X	X	X	X	X	X	X
Run AIDA32 (Print Report)	X			X			X			X		
Clean Inside CPU	X			X			X			X		

This ICT Policy is applicable to the KEWI staff and students and will be updated from time to time to reflect the emerging changes in the Institute. Where clarification of any regulation contained in this manual is required it should be sought from the Director Kenya Water Institute

Approved by the Governing Council for Implementation

……

Dr. Leunita A. Sumba

DIRECTOR/SECRETARY TO THE GOVERNING COUNCIL

FOR: THE GOVERNING COUNCIL

DATED: MARCH 2018