MUHIMBILI UNIVERSITY OF HEALTH AND ALLIED SCIENCES

INFORMATION & COMMUNICATION TECHNOLOGY (ICT) SECURITY POLICY AND PROCEDURES

November 2017

ACRONYMS

CCTV	Closed Circuit Television
CEPD	Continuing Education and Professional Development
DCEPD	Directorate of Continuing Education and Professional Development
DICT	Directorate of Information and Communication Technology
DLS	Directorate of Library Services
E-Learning	Electronic Learning
HEIs	Higher Education Institute
ICT	Information and Communications Technology
IMS	Information Management Systems
ISP	Internet Service Provider
MAC	Media Access Control address
MDGs	Millennium Development Goals
MUHAS	Muhimbili University of Health and Allied Sciences
NSGRP	National Strategy for Growth and Reduction of Poverty
R&D	Research and Development
SOP	Standard Operating Procedures
VPN	Virtual Private Network

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Background

The rapid evolution and growth in the complexity of new systems and networks, coupled with the sophistication of changing threats and the presence of intrinsic vulnerabilities, present demanding challenges for maintaining the security of Information and Communications Technology (ICT) systems and networks.

As a response to such challenges, Information Security standards and procedures are essential to ensure interoperability among systems and networks, compliance with legislation and adequate levels of security. These need to be defined so as to provide the means for protecting the user, creating a more secure and profitable environment for the University and its staff.

In addition, the University information and technology assets are highly valuable and must be closely safeguarded. MUHAS operate within an increasingly electronic, interconnected, and regulated environment that necessitates a consistent and standardised approach to securing technology and information assets.

To ensure the continued protection of MUHAS information and to maintain a secure environment, the management team of MUHAS strongly believes that an ICT security approach aligned with industry standards is necessary.

In view of the above, it is essential for MUHAS staff responsible for planning, acquisition, configuration, deployment, management and auditing of information systems to apply sound risk management practices when selecting security controls. This would include identifying what information is intended to be protected, what are the threats to that information or information system resource and what are the proper cost-effective safeguards that need to be applied to adequately protect the information.

1.2. Rationale

It is the mandate of the University that the information assets are protected from all types of threat, whether internal or external, deliberate or accidental, such that:

i. Confidentiality of information is maintained;
ii. Integrity of information can be relied upon;
iii. Information is available when the business needs it; and
iv. Relevant statutory, regulatory, and contractual obligations are met.

1.3. Purpose and Context

This ICT Security Policy is the cornerstone of MUHAS ICT security program/strategy, aimed at securing the information assets of the university. It is also the purpose of this document to high level directives for individuals or relevant stakeholders to ensure university ICT resources are protected. The policy is based on standard policy framework issued by MUHAS and had taken into consideration other existing university level policies and other National policies for the purpose of ensuring institutional-wise and national policy linkages.

1.4. Scope of Application

This policy and procedures is applicable to all staff and students at MUHAS, visitors as well as providers offering services to MUHAS, all users of ICT equipment owned or leased by the Institution as well as all equipment connected to ICT related infrastructure at MUHAS. In addition, the policy applies to all University's ICT related resources and services.

1.5. Relevant Government Policies and Legislations

The ICT policy and procedures is in-line with the following key policy documents:

i. MUHAS ICT Policy and Procedures (2017)
ii. The Tanzania's National ICT Policy of 2016, which emphasizes the use of ICT to enhance and improve the quality of delivery of education in all areas.
iii. The Education and Training policy (2014) that emphasizes the importance of the application of ICT in the Universities to improve teaching and learning and other related functions.

iv. The Universities Act (2005) which advocates on the need for the availability of adequate CT facilities and services in terms of quality and quantity to support the core functions of the University.
v. Tanzania National Health Policy (2007), Tanzania Development Vision 2025, the National Strategy for Growth and Reduction of Poverty (NSGRP), and the Millennium Development Goals (MDGs).
vi. Tanzania Cybercrimes Act, 2015
vii. Circular No. 3 of 2013 guidelines on the implementation of various ICT systems
viii. Circular No. 5 of 2009 on proper use and ICT security
ix. Circular No. 6 of 2009 on Storage and disposal of information on ICT devices

1.6. Policy Objectives and Outcomes

The objective of this Policy and associated procedures are to:

i. Minimise the exposure of the University to security risks.
ii. Ensure the security of ICT services and facilities, information assets and associated infrastructure.
iii. Provide direction and support for ICT security management

It is expected that when the ICT Security Policy is fully embraced, the following will be realized.

i. Enhanced Users compliance with the relevant ICT procedures, guidelines and standards.
ii. Protected ICT systems deployed by the University.
iii. MUHAS ICT hardware and software adequately secured.
iv. Enhanced disposal of MUHAS ICT equipment.

2. DEFINITION OF TERMS

i. **Cloud computing** - is a technology that uses the internet and central remote servers to maintain data and applications

ii. **Computer Viruses** - is a relatively small software program that is attached to another larger program for the purpose of gaining access to information or to corrupt information within a computer system

iii. **Cybercrime -** is a term for any illegal activity that uses a computer as its primary means of commission

iv. **Data Availability -** refers to how available data is when stored in some form, usually in reference to remote storage of data through a network or external storage media.

v. **Data Confidentiality** - means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

vi. **Data Integrity -** is a term used to refer to the accuracy and reliability of data.

vii. **Encryption**- is the conversion of data into a form, that cannot be easily understood by unauthorized people unless to the intended recipient with a proper coding key.

viii. **End user-** is the person that a software program or hardware device is designed for.

ix. **ICT assets** are defined as equipment with central processing unit such as servers, network appliances, network storage devices, photocopier, scanner, computers, mobile devices, media player, digital cameras, audio-video recorders, large screen displays, projectors, amplifier, video or audio control units, but also include, and not limited to, software, functional support equipment and structure that are considered, part or as a whole, ICT solution.

x. **Media Access Control address** of a computer is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment

xi. **Malicious code** - refers to a broad category of software threats that can cause damages or undesirable effect to computers or networks. System abuse Insider threat

xii. **Disclaimer -** A statement intended to specify or delimit the scope of rights and obligations that may be exercised and enforced by parties in a legally recognized relationship.

xiii. **Phishing attack -** The act of sending email to a user falsely claims to be an established legitimate enterprise in an attempt to steal users' private information that will be used for theft.

xiv. **Spam -** is unsolicited commercial advertisements distributed online. Electronic junk mail or junk newsgroup postings

xv. **Temporary Employee -** refers to a situation where the employee is expected to leave the employer within a certain period of time.

3. POLICY STATEMENTS AND PROCEDURES

The policy statements are presented in six thematic policy issues followed by the operational procedures under each policy statement.

3.1. ICT Security Governance and Management

Effective ICT Governance practices have impact on how security of information assets are achieved at the University. This includes how risks are managed, resources are allocated to implement several security measures as well as university management commitments towards achieving the notable goal of operating in universally secured environment. Thus, special policy provisions are necessary on ICT Security Governance and Management.

3.1.1. Policy Statement 1

The University shall ensure ICT security practices are implemented on discharging its core functions.

Operational Procedures

The University shall:

i. Establish ICT Security Governance Committee
ii. Ensure Changes to the organization, business processes, information processing facilities and systems that affect ICT security shall be controlled.
iii. Ensure ICT security is addressed in all ICT related projects
iv. Allocate sufficient resources for effective ICT security

The DICT shall:

i. Appoint staff who will be a Single Point of Contact (SPOC) for ICT Security Matters
ii. Allocate sufficient resources for effective ICT security management

3.1.2. Policy Statement 2

The University shall ensure a consistent and effective approach is applied to the management of risks and information security incidents on continuous basis.

Operational Procedures

The University shall:

i. Integrate ICT security risk management that include risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and evaluation into the Enterprise Risk Management Framework.

The DICT shall ensure:

i. separation of development, testing, and operational environments to reduce the risks of unauthorised access or changes to the operational environment
ii. the use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance

3.2. Security of ICT Assets

Asset Management involves activities for asset acquisition, storage, usage, maintenance and disposal. The assets include ICT hardware, software, data, system documentation, and storage media, supporting assets such as computer room air conditioners and UPSs. Inappropriate use of ICT assets may expose the University to risks including but not limited to loss of these resources, malware attacks, compromising investment, compromise network systems and services and legal implications.

3.2.1. Policy Statement 3

The University shall ensure that ICT assets are protected for the entire lifecycle of the Asset.

Operational Procedures

The University shall ensure that:

i. All employees and external party users return all ICT assets in their possession upon termination of their employment, contract or agreement.
ii. ICT asset are disposed off securely when no longer required, using the formal procedures established at the University based on issued government directives.

The DICT shall:

i. Ensure all ICT assets are labelled in accordance with the information classification

scheme adopted by the University.

ii. Develop and implemented in guidance for handling ICT assets in accordance with the information classification scheme adopted by the University.

iii. Develop and implemented in guidance for handling removable media in accordance with the information classification scheme adopted by the University.

iv. Ensure that equipment are protected from power failures and other disruptions caused by failures in supporting utilities.

v. Ensure Security measures are applied to off-site ICT assets taking into account the different risks of working outside MUHAS premises.

vi. Ensure all items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

vii. Ensure all servers shall place in a secure room(s) dedicated for such services to be referred to as server room(s).

viii. Ensure all servers of sensitive data must be of sufficient capacity and be of type that ensures stability.

ix. Ensure System administrators given super user status must be vetted for ethics and professionalism.

x. Ensure any system administrator known to have mishandled administrator password shall be replaced immediately, passwords changed and possible ill assigned access rights reviewed and restored.

The head of Units shall ensure that:

i. Equipment are properly maintained to ensure its continued availability and integrity.

ii. Equipment, information or software shall not be taken off-site without prior written authorisation.

3.2.2. Policy Statement 4

The University shall ensure that information held or being processed in an ICT Asset is secured.

Operational Procedures

The University shall:

i. Ensure that every person holding ICT asset is held responsible with information contained in the asset.

The DICT shall:

i. Categorize and classify ICT assets based on sensitivity of Information possessing.
ii. Develop guidelines on Acceptable use of information, assets associated with information and information processing facilities
iii. Ensure Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
iv. Develop and implement cryptographic controls for protection of information and information processing facilities.

The Employee shall

i. Ensure that Media containing information is protected against unauthorised access, misuse or corruption during transportation in and out of University
ii. Not disclose University business information unless authorized to do so
iii. Make data back up regularly

3.3. Access Control and Management

Access control to the University information is a key component in information security management. Access to information, ICT assets and business processes must be controlled on the basis of business and security requirements. All users must be registered, authenticated and access to the MUHAS networks and business systems and use of ICT assets strictly controlled. MUHAS users must be aware of their responsibilities in accessing ICT networks, assets and business systems. Access Control Policy shall prevent unauthorised access to the University's information systems and helps in monitoring and detection of unauthorised activities.

3.3.1. Policy Statement 5

The University shall ensure that access to University ICT services and facilities incorporates

appropriate authentication controls.

Operational Procedures

The DICT shall ensure that:

i. Users of MUHAS Systems only be provided with access to the network and network services that they have been specifically authorised to use.
ii. Authentication where possible, be provided using a unique username and strong password which is assigned to each Authorised User. Password details must be kept secret, and account details must not be shared
iii. A formal user registration and de-registration process shall be implemented to enable and disable assignment of access rights.
iv. A formal user access provisioning process is implemented to assign and revoke access rights for all user types to all systems and services
v. allocation and use of privileged rights is restricted and controlled
vi. Users' access rights of ICT Assets and systems are reviewed at regular intervals

3.3.2. Policy Statement 6

The University shall ensure that the uses of systems are in accordance with the access rights provided.

Operational Procedures

The University shall:

i. Ensure access rights of all staff and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.

The DICT shall

i. Ensure that access to ICT equipment and systems is restricted to authorized users through various systems protection mechanisms
ii. Ensure that users are aware of their responsibilities for maintaining effective access

controls, particularly regarding the use of passwords and the security of user equipment.

iii. Use security systems at network, operating systems and application systems to restrict unauthorized access to computer resources.

iv. Ensure that Logical access to software (applications or data) and information is restricted to authorized users.

v. Ensure that the use of utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.

vi. Ensure that access to program source code is restricted to authorized personnel only

3.4. ICT Physical and Environmental Security

Adequate security must be provided to ensure the protection of physical environment by enhancing facilities for housing, securing and protecting ICT infrastructure. In addition, physical access to the environment and sensitive areas must be restricted in order to protect the confidentiality, integrity and availability of information systems, information and resources.

3.4.1. Policy Statement 7

Critical or sensitive information system facilities shall be housed in secured areas, protected by a defined security perimeter, with appropriate security barriers and entry controls.

Operational Procedures

The DICT shall

i. Ensure equipment, cabling and supporting utilities are protected from interception or damage.

ii. Ensure that equipment are identified and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

3.4.2. Policy Statement 8

Physical access to highly sensitive areas such as Data Centre, server rooms and network control rooms shall be controlled with appropriate identification and authentication.

Operational Procedures

The University shall:

i. Ensure that access points such as delivery and loading areas and other points where unauthorised persons could enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
ii. Ensure that Staff with authorization to enter such areas shall be provided with information of the potential risks involved.

The DICT shall

i. Ensure that security perimeters defined and used to protect information processing facilities and areas that contain either sensitive or critical information.
ii. Ensure secured areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.
iii. Ensure that physical security for offices, rooms and facilities are designed and applied.

3.5. Information Systems Security

The University's business activities need not be interrupted by foreseen and unforeseen events (e.g. natural disasters, technological failures or human error) due to sensitivity of information and services provided to the general public and other institutions. For this to happen, Business continuity management need to be well planned and implemented to minimize the impact on business operation to an acceptable level and facilitate quick recovery of information systems. In this direction, policy commitments are needed to ensure all Strategic Business entities are identified and ensure continued provision of business services.

3.5.1. Policy Statement 9

The University shall institute measures to ensure continual implementations of its core functions without interruption.

Operational Procedures

The University shall:

i. Develop and implement business continuity plans (BCP) and procedures to counteract potential interruptions to critical business processes from the effects of major failures of ICT infrastructure, information systems or disasters, to ensure their timely resumption.
ii. Ensure that Business Continuity Plan is tested and updated regularly to ensure that they are up-to-date and effective and the results to be documented.

The DICT shall

i. Develop Disaster Recovery Plan (DRP) that identifies potential impacts that would threaten the continuity of the University's operations. This will also provide a framework for building resilience and the capability for an effective response which safeguards the interests of the University and of its key stake holders
ii. Ensure that Disaster Recovery Plan (DRP) is tested and updated regularly to ensure that they are up-to-date and effective and the results to be documented.
iii. Ensure Backup copies of information, software and system images are taken and tested regularly as shall be stipulated in DRP.

3.5.2. Policy Statement 10

The University shall institute measures to ensure continual operations of its core Information Systems.

Operational Procedures

The University shall:

i. Ensure that modifications to Information Systems are limited to necessary changes and all changes are strictly controlled.
ii. Establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

The DICT shall

i. Ensure that ICT security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
ii. Ensure that information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification
iii. Ensure that Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
iv. Ensure development of software and systems take in consideration security measures per prevailing Government standards and guidelines.
v. Ensure that Changes to systems within the development lifecycle are controlled by the use of formal change control procedures.
vi. Ensure that business critical applications shall be reviewed and tested when operating platforms changed to ensure there is no adverse impact on organizational operations and ICT security.
vii. Ensure that Principles for engineering secure systems are established, documented, maintained and applied to any information system implementation efforts.
viii. Supervise and monitor the activity of outsourced system development.
ix. Ensure Information systems are regularly reviewed for compliance with the prevailing Government information security standards and guidelines.

3.5.3. Policy Statement 11

The University shall institute Security Incident Management Practices in order to ensure systems are operational on course of implementing its core functions successfully.

Operational Procedures

The University shall:

i. The University shall provide formal procedures for the reporting of information security incidents to management by MUHAS staff, students, visitors, contractors and third party users as quickly as possible.

The DICT shall

i. Ensure systems are monitored to detect deviation from access privileges, record events to provide report and evidence in case of security incidents.
ii. Ensure ICT security events are assessed and it shall be decided if they are to be classified as information security incidents.
iii. Ensure that Knowledge gained from analysing and resolving ICT security is used to reduce the likelihood or impact of future incidents.
iv. Ensure Event logs recording user activities, exceptions, faults and ICT security events are produced, kept and regularly reviewed.
v. Conduct regular security awareness to the MUHAS community

Employees shall

i. Ensure ICT security events are reported through appropriate management channels as quickly as possible.

3.6. Network and Internet Security

With networked or distributed applications, the security of multiple systems as well as the security of the interconnecting network, internet and its services is equally important, especially when public access wide area networks are used. This is due to the fact that while Internet is increasingly becoming a standard working tool for organizations, criminals may target system. This could result in serious loss of confidential information or serious damage to information systems, for example through a premeditated virus attack. To defend against premeditated or opportunistic these attacks, security on the network are to be maintained at the highest level consistent with user needs.

3.6.1. Policy Statement 12

The University shall implement secure and resilient ICT network infrastructure

Operational Procedures

The DICT shall:

i. Keep network secured by minimizing number of network interface points between "secured" network and "non-secured" network;
ii. Keep network secured by separating internal networks and external networks.
iii. Ensure the University network is extended to other external networks without compromising internal security.
iv. Ensure that multiple mechanisms to authenticate user (e.g. password system plus preregistered IP/IPX network plus pre-registered MAC address/terminal number);
v. Manage the network with network management system;
vi. Ensure data is Encrypted with approved encryption algorithm before transmitting over the network.
vii. Ensure that Firewall, and intrusion prevention and detection system are installed and properly configure to protect University network
viii. Ensure that all access points of the network layout are identified, and checks carried out to verify that safeguards are operational.

3.6.2. Policy Statement 13

The University shall ensure that internet use shall not compromise privacy and confidentiality.

Operational Procedures

The University shall

i. Define prohibited websites which should not be visited by staff during working hours and using University's ICT resources.

The DICT shall:

ii. Ensure that Internet connectivity is used for business purposes and that it is used responsibly.

iii. strive to maintain a fast, efficient and secure Internet connection
iv. Ensure that it is protected from harm and danger that come with the use of the Internet.
v. Ensure that it is not the source of harm and danger to the community.
vi. Internet service/connection are not used to perform illegal acts and unauthorised activities.
vii. Ensure that Staff should not access internet using unauthorized Internet devices.
viii. Ensure that all access to the Internet should be routed through web filtering hardware and monitoring software.

Employee shall

i. Browse, access or subscribe to authorized Internet sites that do not contain pornographic, obscene, and immoral or any other inappropriate content.
ii. Ensure that are not use or subscribe to any unauthorized services. This includes chat rooms, computer games and streaming media such as broadcasting services, audio and video streaming.
iii. Abide to Tanzania cybercrime law and regulations when using ICT services at MUHAS.

3.6.3. Policy Statement 14

All official electronic communication shall be made using secured institutional mailing system

Operational Procedures

The DICT shall:

i. Ensure email communications are used responsibly and strictly for official matters.
ii. Ensure that users control spam by using e-mail filtering tools in e-mail software that allow users to block or screen out spam by defining some simple filtering rules.
iii. Ensure that all e-mails from the University e-mail system bear University disclaimer.
iv. Ensure that Mail systems have a mechanism to scan e-mail attachment for viruses and other malicious before sending or downloading.

Employee shall

i. Avoid publishing e-mail address to unknown individuals or exposure of users' credentials by filling forms from dubious links and websites.

ii. Use university e-mail system for official communications.
iii. Avoid replying to spam because most return addresses are not legitimate and would only result in the generation of non-delivery messages thus increasing the amount of undesired traffic.
iv. Use separate e-mail addresses different from their official e-mail addresses when participating in public newsgroup or chat rooms, to avoid their official e-mail addresses and/or mail systems to become a target of spam.
v. Avoid copying or forward e-mails without prior consent of the original sender

3.6.4. Policy Statement 15

Remote access control procedures shall be established to provide adequate safeguards through robust identification, authentication and encryption techniques

Operational Procedures

The DICT shall:

i. Ensure remote access to internal systems is restricted
ii. Thirds party services providers do not access systems remotely without written authorization

4. POLICY STATUS

This is a new policy.

5. KEY STAKEHOLDERS

5.1. The stakeholders who were consulted during revision of this policy include the following:

i. Vice Chancellor, Deputy Vice Chancellors
ii. Deans and Directors
iii. Senate ICT Committee Members and the ICT staff
iv. Staff and Students

5.2. The main stakeholders of this policy are:

i. All MUHAS staff and students
ii. Vice Chancellor, Deputy Vice Chancellors

iii. Deans and Directors
iv. Heads of Departments and Administrative units
v. Staff and Students
vi. Visitors, and service providers/contractors

6. APPROVAL DETAILS

The policy was approved by the University Council at its 46th meeting held on 1st November, 2017.

7. RELATED LEGISLATION

i. MUHAS Institutional Repository policy (2012)
ii. MUHAS Information and Communication Technology Policy (2004)
iii. MUHAS Research Policy (2011)
iv. MUHAS Gender Policy (2013)
v. MUHAS Human Resources Training and Development Policy (2012)
vi. MUHAS HIV/AIDS Policy (2008)
vii. MUHAS Intellectual Property Policy (2011)
viii. MUHAS Library Policy and Procedures (2013)

8. RELATED DOCUMENTS

i. MUHAS University Charter (2007)
ii. MUHAS Student bylaws (2013)
iii. MUHAS Staff Performance and Appraisal Guidelines (2009)
iv. MUHAS Cooperate Strategic Plan (2013/14 – 2017/18)
v. MUHAS ICT Strategic Plan (2015/16 – 2019/20)

9. EFFECTIVE DATE FOR THE POLICY

The policy will be effective upon such date approved by the University Council or such date stated by the University Council for the policy to become effective.

10. NEXT REVIEW DATE

The MUHAS ICT Security policy and procedures will be reviewed after every three years or when deemed necessary to assess the effectiveness of its implementation and determine policy areas that need to be revised. The periodic review will ensure the policy is in line with the

University, national and international changes that might have taken place.

11. POLICY OWNER

The University Council shall own the MUHAS ICT policy.

12. CONTACT PERSON

The contact person for issues related to the ICT policy and procedures shall be:

The Director, Information and Communication Technology (DICT)
Muhimbili University of Health and Allied Sciences
P.O. Box 65001
United Nations Road, Dar es Salaam, Tanzania.
Email: dict@muhas.ac.tz
Telephone: +255 22 2152271 Ext. 1032

ANNEX 1: PASSWORD MANAGEMENT GUIDELINES

This Guideline applies to all staffs that have a username and password to use in at least one system or application at the University, independent of whether you are an end user or a system administrator.

A Strong Password is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

Guidelines for creating a Strong Password:

i. Be at least 8 characters in length
ii. Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
iii. Have at least one numerical character (e.g. 0-9)
iv. Have at least one special character (e.g. ~!@#$%^&*()_-+=)

A Strong Password should not -

i. Spell a word or series of words that can be found in a standard dictionary
ii. Spell a word with a number added to the beginning and the end
iii. Be based on any personal information such as user id, family name, pet, birthday, etc.

How to Maintain a Strong Password:

i. Do not share your password with anyone for any reason
ii. Change your password periodically
iii. Consider using a passphrase as a hint instead of a password
iv. Do not write your password down or store it in an insecure manner
v. Avoid reusing a password
vi. Avoid using the same password for multiple accounts
vii. Do not use automatic logon functionality

Guidelines for Systems Administrators Managing User Accounts:

i. Enforce strong passwords
ii. Require periodic password changes
iii. Require a change of initial or “first-time” passwords
iv. Always verify a user’s identity before resetting a password
v. Never ask for a user’s password Change default account passwords
vi. Implement strict controls for system-level and shared service account passwords
vii. Do not use the same password for multiple administrator accounts
viii. Do not allow passwords to be transmitted in plain-text
ix. Do not store passwords in easily reversible form
x. Implement automated notification of a password change or reset