UNIVERSITY OF DAR ES SALAAM

Computer, Applications and Network Security Management Guideline

Directorate of Information and Communication Technologies

June 2024

Guideline Approval

Document name	Computer and Network Security Management Guideline
Version	UDSM/ICT/CA&NSMG/V1.0_2024
Prepared by	Directorate of Information and Communication Technologies
Owned by	University of Dar es Salaam
Approved by	University Council
Date Approved	
Signature	
Signed by	

Document information

Document Name	Computer, Applications and Network Security Management Guideline
Category	ICT Security
Related policies, standards and guidelines.	• UDSM ICT Policy – Reference to section 3.2 *(Information Systems and Application Software)* • UDSM ICT Security Policy • UDSM Business Continuity and Disaster Recovery Plan • UDSM ICT Master Plan. • UDSM ICT Maintenance Plan. • Identity and Access Management Policy Records & Information Management Policy IT Risk Management Policy • Standard and Guidelines for Government ITCT Project Implementation.
Version number	UDSM/ICT/ CA&NSMG/V1.0_2024

Details of Version History and Authors

V1.0: 01/04/2024	*First Draft Document Submitted for Approval*	*DICT Team*

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BYOD	Bring Your Own Device
CCTV	Closed Circuit Television
CPU	Central Processing Unit
DBMS	Database Management System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DICT	Directorate of Information and Communication Technologies
DNS	Doman Name System
DoS	Denial of Service Attack
DSA	Digital Signatures Algorism
EOL	End of Life
EOS	End of Support
FDE	Full Disk Encryption
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technologies
IDPS	Intrusion Detection and Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
iSCSI	Internet Small Computer System Interface
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NAS	Network Attached Storage
NFS	Network File System
NTP	Network Time Protocol

ODBC	Open Database Connectivity
OS	Operating System
PC	Personal Computer or Workstation
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RSA	Rivest-Shamir-Adleman
SAM	Security Accounts Manager
CVE	Common Vulnerabilities and Exposures
SHA	Secure Hashing Algorithm
SIEM	Security Information and Event management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedures
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SYN	Synchronise
TCP	Transfer Control Protocol
TCRA	Tanzania Communications Regulatory Authority
TLS	Transport Layer Security
TZ-CERT	Tanzania-Computer Emergency Response Team
UDP	User Datagram Protocol
UDSM	University of Dar es Salaam
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

1. INTRODUCTION

1.1. Purpose

This document provides the guidelines for computers, applications and network security management at the University of Dar es Salaam (UDSM). As a guide, it contains security-related information and procedures which must be considered and followed across the University in managing computers, applications and network. The document is part of the implementation of the UDSM Information and Communication Technologies (ICT) Policy objectives as provided in Section 3.8 of the UDSM ICT Policy of 2022; and security principles and statements as provided in the UDSM ICT Security Policy. In the latter, it focuses on Section 4.2 on ICT Security Operations and Communication Management and Section 4.4 on Identity and Access Control Management. The referred sections in both policies call for the guidelines and standard operation procedures (SOPs) for the protection of various system software, application software, devices, hardware equipment and technologies.

1.2. Rationale and Scope

Proper and standardised management procedures for computers and networks across the University is crucial in ensuring service availability and reliability to ICT end-users on the one hand; but also seamless operations and security of the entailed ICT resources of the University on the other hand. Improper management of computers and networks may lead to information security breaches; whereby sensitive institutional information and/or data could be disclosed to unauthorised parties. This is a breach of confidentiality which in itself may lead to other problems for the institution, including damage to the brand and reputation and legal claims among others. On the other hand, currently, there are no such guidelines and therefore management of computers and networks at the University is based on one's understanding of relevant best practices rather than on well-established, standardised and approved guidelines for the same at the University. To avoid the forgoing problems UDSM need to have in place formalised institutional-wide computers, applications and network management guidelines, so as to assist UDSM's units in the proper management of computers and networks which are under their locality. This guideline document supports the implementation of UDSM ICT Policy with regard to the following Policy Objectives and Requirements:

i. To develop, operationalise and enforce ICT Security implementation SOPs.

ii. To acquire appropriate equipment, software and technologies to secure and protect ICT resources.

iii. To secure all ICT resources across campuses.

iv. To strengthen and expand the deployment of directory service.

v. Acquire and deploy a centralised antimalware software to use in all University computers.

The guidelines provided in this document also support the implementation of UDSM ICT Security Policy with regard to the following security principles:

i. to ensure correct and secure ICT operations and communication management of all information processing facilities at the University

ii. to adequately control access to University's critical business information assets and ICT resources.

In particular the guidelines refer to the management of any computer related equipment, computer networks and associated infrastructure components (e.g. servers, storage systems and network devices). It also applies to all physical media which contain confidential information for example: computer storage media such as disks and external hard drive.

1.3. Intended Audience

This document is primarily intended for UDSM staff who are involved in the general management of the security of computers, networks and associated infrastructure and facilities. These may include staff member from the Directorate of ICT (DICT), DICT representatives in different Units of the University, or ICT contractors working for or on behalf of the University.

1.4. Definitions of Key Terms and Concepts

- The term **"UDSM Unit"** refers to any of the various academic or administrative units within the University of Dar es Salaam.
- The term **"Policy"** would mean UDSM ICT Policy 2022 and "Security Policy" would mean UDSM ICT Security Policy 2022 and as amended from time to time. Policy is defined as a high-level statement of organizational beliefs, goals and objectives and the general means for their attainment in a specified subject area.
- **"Software"** - to list all applications in use by the University would be impossible, however software can be summarized as follows:
  - o *Desktop Software* – all applications and related data loaded onto a Desktop or Laptop computer.
  - o *Server Software* – all applications and related data loaded onto a server.
  - o *Hosted Solution* – all applications and related data (owned by UDSM) hosted off site either in the subscribed services e.g. Turnitin, or in any third-party provided Data Centre.
- **Information Security** is the preservation of:
  - o *Confidentiality:* ensuring that information is accessible only to those authorized to have access;
  - o *Integrity:* safeguarding the accuracy and completeness of information and processing methods; and

- *Availability:* ensuring that authorized users have access to information and associated assets when required.

2. WORKSTATION FLEET SECURITY MANAGEMENT

2.1. Introduction

Workstations or computers used by end-users will be managed based on recommended University-wide Workstation Architecture. There are also mobile devices such as smartphones and tablets that are increasingly being used for mainstream work tasks. On the other hand, server computers, which are generally hidden from view in computer rooms, and which provides services or performing computations tasks in the data centre are not workstations.

2.2. Workstation Architecture Elements

- The recommended workstation architecture for the University outlines important issues/elements concerning workstations and provides guidance on the decision to be made about them and their implementation during the rollout stage of workstations as well as during their daily operations. The aim being to ease the management tasks on the part of system administrators; to enhance the availability and reliability of ICT-based services on the part of end users; and also, to ensure the security of ICT resources across the University.
- The primary elements of a workstation architecture are the hardware itself and how it should be made available to end users, the operating system(s), network configuration, the accounts and authorization system, data storage, software updates, host security and events logging.
- The next subsection describes the workstation architecture elements and guides what is expected of each of them.

2.2.1. Fungibility Concept

To a feasible extent, workstations should be deployed and configured in such a way that they become a fungible resource. Thus can easily be replaced with another workstation or mutually interchangeable.

Guidelines

i. In University units, any one workstation should be able to substitute for any other in the given settings.

ii. It should be possible for anyone with UDSM account to log into any workstation connected to the University network to improve access locality, especially in a large desktop environment.

iii. If a user logs into someone else's computer, should not be able to access that person's files

iv. The applications that are needed by the end users in the unit should be immediately available.

v. Users' files should be stored on network file servers, not in local disk, so that they are accessible from anywhere.

vi. Operating systems and application programs should be updated automatically with minimal or no user involvement.

vii. A user of a workstation should be able to customize it but not break it or subvert its security.

The ability to log into any workstation improves access locality. This is especially useful in a large desktop environment, which allow user to log in and computer and access his workspace.

2.2.2. Hardware

Selecting physical hardware such as laptops, desktops, tablets, smartphones and other mobile devices, is the most fundamental choice to be made by an institution. Several factors can be used to choose devices to use.

Guidelines

i. The University or unit should make a decision on whether to deploy physical workstations, virtual workstations, or both.

ii. The University or unit should specify workstations based on different categories and or groups of users .

iii. Establish whether workstations are wholly provided by the University or bring your own device (BYOD) strategy is to be employed

iv. Establish hardware requirements for different categories of users within the University (E.g., some users need laptops while others need desktops; and others may require workstations with additional RAM, faster CPUs and larger hard drives or screens.

2.2.3. Operating Systems (OS)

- An operating system is a software layer between the computer applications and hardware as a mediator that enables and coordinates applications to share computer resources.
- The University workstation architecture, should be constituted by a single or multiple operating systems depending on the actual use of a given workstation. Major OS groups such as Microsoft Windows, Apple OSX and Linux, are mainly categorised by vendors producing them, each with small variations within the group. For example: Linux has both different vendors and versions within those vendors. For example, Red Hat, Ubuntu, Debian, CoreOS and other vendors make Linux distributions ("distros") by packaging the

Linux kernel with different sets of applications, utilities and enhancements. Each distro releases major new versions periodically, with minor updates being provided in between.

- Similarly, Microsoft and Apple have server and workstation variations of each operating system. Server editions are bundled with additional features and capabilities or tuned with different defaults.

Guidelines

i. For the proprietary OS such as Windows only genuine and licensed copies approved or provided by DICT shall be installed in the University workstations. OS can also be specified during the procurement of new workstations in which case it will come already installed in the procured workstations. However, verification of whether the supplied OS is genuine or not should be done during the delivery of the goods

ii. Usage of open-source OS (e.g. Ubuntu) in the University workstations should be recommended. DICT will identify and select open-source OS to be used at the University

Notice

- The decision of whether to support one or many operating system groups within the University may be similar to that of whether to support different hardware models.
- The University should minimize the use of different hardware and software to simply support. Standardising on one type of OS or hardware does not only simplify the provision of the needed support but also the procurement process.

2.2.4. Network Configuration

- Workstations are connected to a network by either wired (Ethernet) or wireless (Wi-Fi) technologies.
- The decision to be made whether the network configuration has to be hardcoded/static (stored on the machine itself) or dynamic (provided by the network). These configuration parameters include the machine’s IP address, subnet netmask, default gateway, DNS servers and more.

Guidelines

i. Unless a situation warrants otherwise, all workstations' network interfaces should be configured to receive IP dynamically from the network.

ii. Machines (e.g. servers, shared printers) which provide service to other machines should use static IPs

2.2.5. Accounts and Authorization

- Workstations need a database of usernames, passwords, groups and related account information. Architecturally, the decision must be made whether this information is stored on the machine itself, accessed from a central database over the network, or both.
- All machines have a local account database. Unix based systems have etcpasswd and etcgroup. Windows systems store local accounts in the Security Accounts Manager (SAM).
- When account information is made available as a network service, it is generally called a network directory. The most common example is Microsoft Active Directory, though there are others such as Apple's Open Directory and Red Hat Directory Server. All of these are based on the LDAP protocol for database-like access to this information and Kerberos for the secure handling of passwords and authentication.

Guidelines

i. Each workstation must be joined to a network directory service (i.e. a University Active Directory domain). Since a directory stores usernames and passwords of the list of machines or the accounts permitted to log into, users can use the same username and password on any (permitted) machine.

ii. By default, each normal user must be configured without administrative access.

iii. If a user of a given workstation leaves the University, his/her account must be disabled in the directory.

iv. Access policies must be stored in the directory. Storing access policies in a directory means they are applied consistently everywhere. A policy might exclude other machines which are designated for use by particular University members of staff exclusively

v. A Local account database for workstations must be maintained. While network directory services are important, local account databases still have their place. One benefit of a local account database is that the information is always available, whether or not the machine is connected to a network and even if the network directory server is down. For example, being able to log into a local administrator account whose credentials are stored in the local account database is often required to fix a damaged or misconfigured machine that is unable to talk to the network. The ability to store different information in the local account database of each machine has benefits.

vi. Where Administrative Access has been requested and granted, a record of this must be kept in an appropriate register for auditing, reporting and review purposes.

vii. Administrative access may only be granted where one of the following exceptions apply:

a. Where staff are required to use specialised applications which require administrative access to function correctly.

b. Where staff carry out IT development work involving software and/or hardware (or as part of research or teaching activities.

c. Where staff perform other special roles where the DICT deems that the nature of their work requires Administrative Access.

viii. Administrative Access is only to be granted at the discretion of the DoICT.

2.2.6. Data Storage

The user of a workstation needs to store information, or state. Generally, this is in the form of files and directories but also includes configuration and customizations that users make to their environment. There are three fundamental ways to configure storage:

- **Local:** All data files are stored locally. The system is configured so that the user's files are stored on the local disk, which is also used to store the OS and any OS-related files and state. Local storage is generally the default for most operating systems. Local storage is simple to set up and always accessible. The primary drawback to local storage is that it is risky if the Disks fail, or users accidentally delete data. Therefore, such data needs to be backed up.
- **Stateless:** No locally unique data. Users' files are stored remotely on a network server (remote file storage). Any information that is stored locally is a copy of data that is stored elsewhere. The local disk is used only for the OS, temporary files and caches. Ideally, if the local disk was wiped, the only information that would be lost would be disposable temporary files and cached copies of files whose master copies are stored on the remote server.
- **Diskless:** No local disk storage. The operating system and user data are stored on a remote disk over a network using protocols such as iSCSI or NFS. If the machine dies, the same chunk of storage can be attached to a replacement machine. This setup is most commonly used in virtual machines and blade systems.

Guidelines

i. University shall provide network storage service (centralised file storage) for all members of Staff.

ii. All University workstations must be configured to use both local storage and remote file storage i.e., government cloud storage whereby users' files are stored locally but copied to a network service as soon as possible.

2.2.7. OS and Application Software Updates

Once an OS is installed, it is essential to apply needed patches or upgrades to fix known vulnerabilities. As long as software is being actively supported by the vendor, there will always be updates/patches that add new features, fix bugs and or close security holes. Keeping machines up-to-date is part of good system hygiene. Hence, one must have a strategy for how software updates will be deployed. Important considerations to be made here are the following:

- how software updates are done and approved,
- when updates should happen and how frequent

NB: Updates can be installed manually or automatically.

i. **The manual Method**: Systems administrators (sysadmin) at the University should access each machine and give the commands to install the updates, possibly rebooting the machine if that is required. This can be done either physically or through remote access mechanisms such as Remote Desktop Protocol (RDP) or Secure Shell (SSH).

ii. **The Automatic Method**: A machine is configured by the systems administrator to perform the upgrades without system administration intervention or configuration can be done from the update server side.

Guidelines

i. OS and Application software installed in all University workstations must be kept up-to-date by regularly updating them according to agreed schedules

ii. Any known vulnerabilities for a given OS should be fixed in all affected computer hardware before they are used in the University production environment.

iii. To reduce bandwidth consumption for updates download which at times might involve substantially large files, a dedicated machine shall be set in a University network for pulling all the desired updates for OS and other application software from the sources and then distribute them locally to all workstations at the University.

iv. Distribution of the updates should be controlled centrally to allow decisions such as which patches are to be distributed, to which specific workstations.

v. Incremental (regular) updates should be automated to happen without the intervention of user or sysadmins.

vi. Major updates (Feature updates) must be tested before they are deployed across the University.

vii. A dashboard managed by systems administrator at the University should be in place to display which machines have not been upgraded. Such machines should be tracked down to identify the cause of the delay.

viii. Designated systems administrator at the University should have the ability to stop all updates if a problem is detected.

ix. Systems administrators at the University should be able to rapidly deploy a specific update in an emergency.

x. All OS and Application software that have reached End of Support (EOS) or End of Life (EOL) status must be removed from use in the University ICT environment.

2.2.8. Security

The workstation architecture has many security-related implications, including the ones which have already been covered in this document such as accounts and authorization policy and the ability to distribute security updates. There is also the need to defend machines against data theft, malicious software and changes to the network firewall configuration

i. **PC Theft:** If a University laptop is lost or stolen, the first priority is to make sure that whoever possesses the device cannot access the contents. We would also like to recover the device. But this is not always possible Available alternatives for recovering from a PC theft are:

   a. *To use Laptop tracking software which periodically announces the machine's Mac address and thus helps in tracking its location. If the device is missing, the service can help in locating the machine. Such software often has a remote-wipe feature, which is a way to instruct the lost machine to erase its contents. Some tracking software will enable cameras and microphones and send periodic updates that help you track the device.*

   b. *To use full disk encryption (FDE). FDE encrypts the hard disk in a way that, without the decryption passphrase, makes the data on it basically unusable.*

ii. **Malware:** is software created to insert itself on a machine to subvert the security of the system. Often this takes the form of making use of resources or stealing information. Malware goes by many names: virus, Trojan, backdoors, spyware and so on. Anti-malware is software that detects these programs and disables and reports their existence. Anti-malware software comes in three general categories:

   a. ***Standalone Host Control:*** *Security defence software should be installed and configured in each workstation. A user may be able to make adjustments including disabling the software if has elevated access rights in the workstation.*

   b. ***Centralized control:*** *Security defence software should be configured and controlled from a central point. The user may be able to make some adjustments but not disable the software.*

   c. ***Centralized reporting:*** *There should be a central dashboard that reports the statuses of all machines. This might include which viruses have been detected when the machine received its most recent antivirus policy update, and so on. Knowing when the machine last checked in is key to knowing if the software was disabled.*

Guidelines

i. DICT shall benchmark various reputable anti-malware software products and then select and purchase the one with the least performance impact on the network and the host machine, for use across the University.

ii. Each workstation at the University must be protected from malware using the product recommended by the DICT.

iii. DICT should ensure that malware control and reporting must be done from a central point.

iv. DICT may identify, procure and deploy tools and utilities for protection against theft.

2.2.9. Logging

A workstation architecture needs to make workstations observable. This is done by logging events and making this information accessible. We cannot see everything going on inside a machine, and if we could, trying to watch every machine ourselves, 24 hours each day, does not scale well. Instead, machines log various information as they operate in their environment:

- They log which programs ran, problems and errors, security policy violations and more. These log events need to be collected. Microsoft Windows calls this the event log, and Unix/Linux systems call it the system log, or syslog.
- Logs are recorded to disk locally and can be accessed using various log viewing programs. Another strategy is to forward a copy of all log entries to a central machine for centralized storage, management and viewing. This way we have global visibility from one seat.
- Storing logs centrally enables more sophisticated analysis. One can observe a single person moving from machine to machine or determine the earliest date a particular problem first occurred and correlate it to another event, such as a software upgrade.

NB: Log Analysis Tools: There are many log analysis tools such as *Logstash* and *Splunk* that store and interpret log information. Normally, large environments like the one at the University, use a hub-and-spoke model. Each group of machines forwards a copy of their logs to a hub. There may be one hub per building or University unit division. Then all the hubs consolidate the logs and send them to a central repository for analysis.

Guidelines

i. ICT resources may be monitored by authorised members of DICT, or authorised third parties contracted by and on behalf of DICT.

ii. Logs should be kept secure and are only available to authorised IT users and will only be kept as long as necessary, in line with current data protection guidelines.

iii. Logs will be retained for as long as required by applicable law and or relevant UDSM policy.

iv. IT resources may be monitored and logged for all lawful purposes including:

   a. *tracking the flow of network traffic.*
   b. *facilitating and improving capacity planning*
   c. *identifying areas for improvement, including provision of teaching and learning facilities*
   d. *maintaining good availability of network bandwidth*
   e. *ensuring that the use of resources is authorised*
   f. *management of systems*
   g. *protecting against unauthorised access*
   h. *ensuring system security*
   i. *compliance with University policies and regulations and any other appropriate regulation*
   j. *avoiding or mitigating legal liabilities and complying with legal obligations*
   k. *preventing and detecting crime*
   l. *recording the date/time of transactional-based events*

3. SYSTEMS AND APPLICATIONS ACCESS MANAGEMENT STANDARDS

3.1. Application

This guideline applies to all users, whether physically located at the University or elsewhere but accessing University systems and applications.

3.2. Purpose

To define guidelines of system and application access management at the University, which includes authentication that systems and applications must use. This makes it easier for application owners and implementers to deliver high-quality services that can determine the identity of a user and manage known authentication security risks.

3.3. Definition of User Groups

Before any user could be granted access to a given University system or application, normally users and groups are defined based on user roles and responsibilities.

Guidelines

i. System owners at the University must define the user groups that are allowed access to their applications.

ii. All user access to services, data and functionality must be based on the principle of least privilege.

iii. When a user's role within the University changes, their access must be reviewed and modified as required.

iv. When a user is no longer entitled to belong to a group that allows access to an application, that access must be removed. In the case of involuntary termination, access is to be removed immediately.

v. If it is detected that an account has been accessed in violation of University policies then that account may be disabled without warning.

vi. Applications at the University that need to collect and manage identity information must be protected and consume the required information from central identity management services.

vii. Access control to systems at the University will vary according to the business rules established by the system owners, this must include, where appropriate, rules for segregation of duties.

viii. All systems at the University should have a minimum of two user accounts that are capable of administering the system.

3.4. Issuing and Managing Privileged Access Accounts

At some points, some users of University systems or applications might need to have privileged access accounts to systems or applications. In such scenarios, the following guidelines will be followed:

Guidelines

i. Privileged access will be granted to the user of the account and that person will be designated as the owner of the account.

ii. The owner is accountable for all actions taken under that account.

iii. Documented processes for granting, reviewing and revoking privileged accounts must be maintained. DICT shall ensure the existence of such a documented process as they deem it fit.

iv. The business owner of the system being accessed is the process owner.

v. Privileged access accounts must be approved prior to being configured.

vi. Approval and configuration of accounts must follow the principles of segregation of duties.

vii. All user access to services, data and functionality must be based on the principle of least privilege.

viii. Privileged access may be used only for the duration of time necessary to perform administrative duties. At all other times, standard user access account will be used.

ix. Privileged access accounts must adhere to University password policies and guidelines and be configured for multi-factor authentication.

x. When a user is no longer entitled to privileged account access, such access must be removed immediately.

xi. Monitoring and auditing of privileged accounts will occur on a regular basis.

xii. Monitoring and auditing must follow segregation of duties principles.

xiii. If it is detected that an account has been accessed or used in violation of University policies, then that account may be disabled without warning.

3.4.1. University Systems and Applications User Authentication

Access to a University system or application requires a user to be authenticated first. Authentication establishes the identity of the user when accessing systems and applications. The authentication process provides identity attributes and enables authorisation and personalisation decisions to be made by systems and applications. These decisions help to ensure that users receive access to only the information and transactions to which they are entitled.

Credentials are methods used by an individual to authenticate his or her identity when accessing applications, systemsand online services. Examples of credentials include passwords, one-time passwords, software tokens, hardware tokens and biometrics. Important considerations to be made here are the following:

- **Single Sign-On:** allows an individual to authenticate on entry to a work session and gain access to multiple related but independent University systems and applications.
- **Two-Step Verification:** also known as 2-factor authentication or 2FA, is a security mechanism that requires two types of credentials for authentication and is designed

to provide an additional layer of validation, and hence a possibility of minimizing security breaches.

Guidelines

i. Access to all University applications and systems that contain restricted data and/or confidential data must use some form of authentication.

ii. University must have in place an authentication system or platform that allows single sign-on and multi-factor authentication; in which the first authentication method uses something known to a user (e.g. a password) and the second method uses something the person has (e.g. a token that provides a one-time code).

iii. Where authentication is required, all University web-based applications must use the Single Sign-On platform, except where the application does not support single-sign on.

iv. All authentication attempts into University applications and systems through either the University Single Sign-On platform or other forms of authentication must be logged and reportable.

v. Systems that store or use restricted or confidential data must never be configured to allow access using shared or anonymous accounts.

vi. The strength of authentication implemented in an application must always be suitable for the classification level of the information being accessed and the activities being carried out, such as those that carry financial or reputational risk – e.g. tempering with exam results. All applications or systems with restricted data must have Two-Step Verification enabled.

vii. Generic or shared accounts and credentials must not be used.

3.4.2. Two-Step Verification Authentication

- For users of University systems and applications who are required to authenticate through Two Step Verification continually throughout the day, it may be simpler to use a hard token which requires them to push one button, rather than a soft token which may require more effort.
- Hard tokens (also known as security token) are a small hardware device that the user carries which plugs into a computer and delivers a one-time password to authorise access to online services. Used with a standard username and password, the hard token can provide Two-Step Verification to a site, service or application.
- Soft tokens (also known as software tokens) are Two-Step Verification applications that can be installed and run from a wide variety of devices, including but not limited to personal computers and smartphones. Tokens are used to prove one's identity electronically in addition to a password. The token acts like an electronic key to access something.

Guidelines

i. Applications, systems and services where restricted data is maintained must have Two Step Verification implemented. This requirement must be taken into account during the high-level design, implementation or upgrade of applications and services.

ii. Any system configured for Two Step Verification is to be configured to work with both hard tokens and soft tokens.

iii. Self-Service options that allow users to manage their own tokens are to be strategically prioritised over assisted options, such as those provided by support teams.

iv. All users must be able to authenticate through Two Step Verification where the service has been enabled.

v. If a user leaves or changes role, the systems and services which they are authorised to access, including those where Two Step Verification is enabled, must be adjusted in a timely manner to reflect the change in relationship with the University.

vi. As a part of Token Management and Control, a user must not share their token with another person and hard tokens must be stored securely.

vii. Hard tokens should not be left openly on a desk or plugged into a computer when the user is not present.

viii. If any user reports their Two Step Verification token as lost, stolen, or otherwise compromised their token must be locked, unlinked or deleted as appropriate. This applies equally to soft tokens and hard tokens.

ix. Issued tokens must be returned to the University when they are no longer required.

x. It is recommended that all users who are database administrators or server administrators to use a hard token. Users who do have a smartphone must use a soft token.

4. SERVER SECURITY MANAGEMENT GUIDELINES

4.1 Purpose

The purpose of this guideline is to assist those with responsibilities of managing various University's servers in understanding the fundamental activities they are supposed to perform as part of securing and maintaining the security of servers that provide services over network communications as a main function.

4.2. Scope

There are different categories of servers, for the sake of scope, hosts that incidentally provide one or a few services for maintenance or accessibility purposes, such as a remote access service for remote troubleshooting, are not considered servers in this document. The types of servers which this guideline addresses include all outward-facing publicly accessible servers which University uses to provide services, such as web and email services and a wide range of inward-facing servers. This guideline outlines and discusses the need to secure servers; and provides recommendations for selecting, implementing and maintaining the necessary security controls.

The guideline is meant to address common servers that use general operating systems (OS) such as Unix, Linux and Windows. Many of the recommendations in this document may also be applicable to servers that use specialised OSs or run on proprietary appliances. Conversely, highly specialized servers, particularly security infrastructure devices (e.g., firewalls, intrusion detection systems) and virtual servers - which have unusual configurations and security needs - are outside the scope of this guideline.

4.3. Audience

This document has been created primarily for system administrators and designated security administrators (if any) who are responsible for the technical aspects of securing UDSM servers. The material in this document is technically oriented, and it is assumed that readers have at least a basic understanding of system and network security.

4.4. Preliminary Steps and Activities for Server Security

4.4.1. Server Vulnerabilities, Threats and Environments

To secure a server, it is essential to first define the threats that must be mitigated. Knowledge of potential threats is important to understanding the reasons behind the various baseline technical security practices presented in this SOP. Many threats against data and resources are possible because of mistakes—either bug in operating system and server software that create exploitable vulnerabilities, or errors made by end users and administrators.

Threats may involve intentional actors (e.g., attacker who wants to access information on a server) or unintentional actors (e.g., administrator who forgets to disable user accounts of a former University employee/student.) Threats can be local, such as a disgruntled employee, or remote, such as an attacker in another geographical area. Hence it is important to conduct risk assessments to identify the specific threats against University servers and determine the effectiveness of existing security controls in counteracting the threats; they then should perform risk mitigation to decide what additional measures (if any) should be implemented, Performing risk assessments and mitigation helps the University to better understand its security posture and decide how its servers should be secured.

An important element of planning the appropriate security controls for a server is understanding the threats associated with the environment in which the server is deployed and security needs usually associated with such environments.

4.4.2. Security Categorization of Information and Information Systems

Determining how strongly a system needs to be protected is based largely on the type of information that the system processes and stores. For example, a system containing student's records probably needs much stronger protection than a computer only used for viewing publicly released documents. This is not to imply that the second system does not need protection; every system needs to be protected, but the level of protection may vary based on the value of the system and its data.

For the sake of security categorization of University information and information systems, the following guidelines must be followed:

i. The potential impact is considered to be **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on UDSM - operations, assets, or staff and students. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:
   a. *cause a degradation in mission capability to an extent and duration that UDSM is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;*
   b. *result in minor damage to UDSM assets;*
   c. *result in minor financial loss; or*
   d. *result in minor harm to individuals.*

ii. The potential impact is considered to be MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on UDSM operations, assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:
   a. *cause a significant degradation in mission capability to an extent and duration that UDSM can perform its primary functions, but the effectiveness of the functions is significantly reduced;*
   b. *result in significant damage to UDSM assets;*
   c. *result in significant financial loss; or*
   d. *result in significant harm to individuals, but does not involve loss of life or serious life-threatening injuries.*

iii. The potential impact is considered to be HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on UDSM operations, assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

a. *cause a severe degradation in or loss of mission capability to an extent and duration that the UDSM is not able to perform one or more of its primary functions;*
b. *result in major damage to UDSM assets;*
c. *result in major financial loss; or*
d. *result in severe or catastrophic harm to individuals, involving loss of life or serious life-threatening injuries."*

Guidelines

i. Each system, including all servers that are part of the system, should be protected based on the potential impact on the system of a loss of confidentiality, integrity, or availability.
ii. Security weaknesses in the system need to be resolved.
iii. The system should offer only the required functionality to each authorized user, so that no one can use functions that are not necessary.
iv. Security controls should be implemented in such a way that there is a balance between security, functionality and usability; since security controls often make systems less convenient or more difficult to use.
v. Security protection should use multiple layers of security controls—defence in depth.

4.4.3. Basic Server Security Steps

A number of steps are required to ensure the security of any server. The following steps are recommended for server security

i. Plan the installation and deployment of the operating system (OS) and other components for the server.
ii. Install, configure and secure the underlying OS.
iii. Install, configure and secure the server software with only required services.
iv. For servers that host content, such as Web servers (Web pages), database servers (databases) and directory servers (directories), ensure that the content is properly secured.
v. Employ appropriate network protection mechanisms (e.g., firewall, packet filtering router and proxy).
vi. Employ secure administration and maintenance processes, including application of patches and upgrades, monitoring of logs, backups of data and OS and periodic security testing.

4.4.4. Security Principles Recommended for Server

When addressing server security issues, it is important to keep in mind the following general information security principles:

i. **Simplicity—**Security mechanisms (and information systems in general) should be as simple as possible.

ii. **Fail-Safe—**if a failure occurs, the system should fail in a secure manner, i.e., security controls and settings remain in effect and are enforced.

iii. **Complete Mediation—**Rather than providing direct access to information, mediators that enforce access policy should be employed.

iv. **Open Design** —System security should not depend on the secrecy of the implementation or its components.

v. **Separation of Privilege—**Functions, to the degree possible, should be separate and provide as much granularity as possible. The concept can apply to both systems and operators and users. In the case of systems, functions such as read, edit, write and execute should be separate. In the case of system operators and users, roles should be as separate as possible. For example, if resources allow, the role of system administrator should be separate from that of the database administrator.

vi. **Least Privilege—**this principle dictates that each task, process, or user is granted the minimum rights required to perform its job. By applying this principle consistently, if a task, process, or user is compromised, the scope of damage is constrained to the limited resources available to the compromised entity.

vii. **Psychological Acceptability—**Security mechanisms in place should present users with sensible options that give them the usability they require on a daily basis.

viii. **Least Common Mechanism—**When providing a feature for the system, it is recommended to have a single process or service gain some function without granting that same function to other parts of the system.

ix. **Défense-in-Depth—**Security mechanisms (defences) should be layered so that the compromise of a single security mechanism is insufficient to compromise a host or network.

x. **Work Factor—**The amount of work necessary for an attacker to break the system or network should exceed the value that the attacker would gain from a successful compromise.

xi. **Compromise Recording—**Records and logs should be maintained so that if a compromise does occur, evidence of the attack is available to the University for subsequent measures.

4.4.5. Server Security Planning

The most critical aspect of deploying a secure server is careful planning before installation, configuration and deployment. Careful planning will ensure that the server is as secure as possible and in compliance with all relevant UDSM policies. Experience shows that server security and performance problems can be traced to a lack of planning or management controls, on the one hand; and having a highly fragmented IT support structure on the other. The importance of management controls cannot be overstated. Fragmentation in IT support provision leads to inconsistencies, and these inconsistencies can lead to security vulnerabilities and other issues.

Having a well-prepared deployment plan helps in maintaining secure configurations and aids in identifying security vulnerabilities, which often manifest themselves as deviations from the plan.

4.4.6. Server Installation and Deployment Planning Guidelines

Server installation and deployment should be based on a well-established and documented plan. Security should be considered from the initial planning stage at the beginning of the systems development life cycle to maximize security and minimize costs. In the planning stages of a server, the following items should be considered:

Guidelines

i. Identify the purpose(s) of the server.

ii. Identify information categories which will be stored on the server

iii. Identify information categories which will be processed on or transmitted through the server

iv. Identify the security requirements for this information in (ii) and (iii) above

v. Establish whether any information will be retrieved from or stored on another host (e.g., database server, directory server, Web server, Network Attached Storage (NAS) server, Storage Area Network (SAN) server, etc.)

vi. Identify the security requirements for any other hosts involved

vii. Identify other service(s) which will be provided by the server (in general, dedicating the host to only one service is the most secure option)

viii. Identify the security requirements for these additional services

ix. Identify the requirements for continuity of services provided by the server, such as those specified in continuity of operations plans and disaster recovery plans

x. Identify the location where the server will be located on the network

xi. Identify the network services that will be provided on the server, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Network File System (NFS), or database services (e.g., Open Database Connectivity [ODBC]).

xii. Identify the network protocols to be used for each service (e.g., IPv4, IPv6).

xiii. Identify any network service software, both client and server, to be installed on the server and any other support servers.

xiv. Identify the users or categories of users of the server and any support hosts.

xv. Determine the privileges that each category of user will have on the server and support hosts.

xvi. Determine how the server will be managed (e.g., locally, remotely from the internal network, remotely from external networks, etc.).

xvii. Decide if and how users will be authenticated and how authentication data will be protected.

xviii. Determine how appropriate access to information resources will be enforced.

xix. Determine which server applications meet the UDSM's requirements. Consider servers that may offer greater security, albeit with less functionality in some instances. Some issues to consider include—

  a. *Cost*
  b. *Compatibility with existing infrastructure*
  c. *Knowledge of existing employees*
  d. *Existing manufacturer relationship*
  e. *Past vulnerability history*
  f. *Functionality.*

xx. It may be necessary to work closely with manufacturer(s) in the planning stage if there are such agreements at the University.

xxi. The choice of server application may determine the choice of OS. However, to the degree possible, server administrators should choose an OS that provides the following:

  a. *Ability to granularly restrict administrative or root level activities to authorized users only*
  b. *Ability to granularly control access to data on the server*
  c. *Ability to disable unnecessary network services that may be built into the OS or server software*
  d. *Ability to control access to various forms of executable programs, such as Common Gateway Interface (CGI) scripts and server plug-ins for Web servers, if applicable*
  e. *Ability to log appropriate server activities to detect intrusions and attempted intrusions*
  f. *Provision of a host-based firewall capability to restrict both incoming and outgoing traffic*
  g. *Support for strong authentication protocols and encryption algorithms*

4.4.7. Server Physical Security

UDSM's servers normally host sensitive information, and some others, such as public-facing Web servers, should be treated as sensitive because of the damage to the UDSM's reputation that could occur if the servers' integrity is compromised. In such cases, it is critical that the servers are located in secure physical environments. When planning the location of a server, the following standards should be considered and apply:

Guidelines

i. There should be appropriate physical security protection mechanisms in place for the server and its networking components (e.g., routers and switches). Examples of protections include—

   a. Locks

   b. Card reader access

   c. Security guards

   d. Physical intrusion detection systems (e.g., motion sensors, cameras).

ii. There should be appropriate environmental controls so that the necessary humidity and temperature are maintained. If high availability is required, there should also be redundant environmental controls.

iii. A backup power source should be in place, and its capacity in terms of the number of hours it can provide power, should be known.

iv. There should be appropriate fire containment equipment.

v. There should be an alternative data centre that can be used to host servers in the event of a catastrophe at the original data centre.

4.4.8. Server Management

Appropriate management guidelines are critical to operating and maintaining a secure server. The University should ensure the security of a server and the supporting network infrastructure.

Guidelines

i. Adherence to UDSM's ICT security policy throughout the process of server installation, configuration, deployment and day-to-day operations.

ii. **Configuration/Change Control and Management**: There should be mechanisms for configuration control because it leads to consistency with the organization's information system security policy. Consider the use of development, quality assurance, and/or test environments so that changes can be vetted and tested before deployment in production. Configuration/Change Control and Management is the process of controlling modification to a system's design, hardware, firmware, and software provides sufficient assurance that the system is protected against the introduction of an improper modification before, during, and after system implementation.

iii. **Documentation:** Systems must be operated with the documented configuration and in a manner that provides the best operational performance while applying the greatest information security. Documentation should be current, maintained in a central location and accessible to staff. The level of documentation should be sufficient to:

   a. Prevent a dependency on a single key staff member

b. *Provide serial numbers or license keys needed for installation and vendor support*

c. *Test procedures to minimize downtime when changes occur*

d. *Transmit knowledge to others*

e. *Provide the most current documentation*

iv. System **audit logs**: System audit logs should be configured, and their operation verified immediately on initial system setup. Operational audit logs are maintained on a best effort basis equivalent to 120 days. Logs are reviewed by staff and discrepancies are investigated and resolved as necessary. Systems are configured to generate and centrally store all relevant logs off system. Wherever it is possible, controls and activity auditing should be implemented over the use of utility programs that may provide users the ability to override existing system and application controls.

v. **Risk Assessment and Management:** DICT should ensure that risk assessment and management activities are in place and operational as required. **Risk assessment** is the process of analysing and interpreting risk. Collecting and analysing risk data requires identifying assets, threats, vulnerabilities, safeguards, consequences and the probability of a successful attack. **Risk management** is the process of selecting and implementing controls to reduce risk to a level acceptable to the University.

vi. **Standardized Configurations**: DICT should develop standardized secure configurations for widely used OSs and server software at the UDSM's environment. This will provide recommendations to server and network administrators on how to configure their systems securely and ensure consistency and compliance with UDSM ICT security policy.

vii. **Secure Programming Practices:** UDSM should adopt secure application development guidelines to ensure that all the applications developed for servers, are developed in a sufficiently secure manner.

viii. **Security Awareness and Training**: DICT should arrange, coordinate and facilitate provision of security awareness and training across the University as needed. A security training program is critical to the overall security posture of the University. Making users and administrators aware of their security responsibilities and teaching the correct practices helps them change their behaviour to conform to security best practices. Training also supports individual accountability, which is an important method for improving information system security.

ix. **Contingency, Continuity of Operations and Disaster Recovery Planning**: Contingency plans, continuity of operations plans and disaster recovery plans should be established in advance to allow an organization or facility to maintain operations in the event of a disruption.

x. **Certification and Accreditation:** information system security should be analysed to determine how well it meets all of the security requirements of the University, hence being certified. When UDSM management accepts that the information system meets its security requirements then the system should be accredited.

4.4.9. System Security Plan

The objective of system security planning is to improve protection of information system resources. Plans that adequately protect information assets require that the responsible information owners—directly affected by and interested in the information and/or processing capabilities—to be convinced that their information assets are adequately protected from loss, misuse, unauthorized access or modification, unavailability and undetected activities.

The purpose of the system security plan is to provide an overview of the security and privacy requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behaviour of all individuals who access the system and should be viewed as documentation of the structured process of planning adequate, cost-effective security protection. It should reflect input from various University officials with responsibilities concerning the system, including information owners, the system owner and the DICT.

Guidelines

i. All UDSM's information systems must be covered by a system security plan.

ii. The information system owner is responsible for ensuring that the security plan is developed and maintained, and that the system is deployed and operated according to the agreed-upon security requirements.

iii. In general, an effective system security plan should include the following:

   a. *System Identification—this provides basic identifying information about the system. it includes general information such as the key points of contact for the system, the purpose of the system, the sensitivity level of the system, and the environment in which the system is deployed, including the network environment, the system's placement on the network, and the system's relationships with other systems.*

   b. *Controls—DICT should put in place security control measures that meet protection requirements of the information system. Controls fall into three general categories:*

      - *Management controls, which focus on the management of the computer security system and the management of risk for a system.*
      - *Operational controls, which are primarily implemented and executed by people. They often require technical or specialized expertise, and often rely upon management activities as well as technical controls.*
      - *Technical controls, which are security mechanisms that the computer system employs. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the University.*

4.4.10. Securing the Server Operating System

- It is important that the OSs underlying the servers are configured appropriately. A server administrator needs to configure new servers to reflect established UDSM's security requirements and reconfigure them as those requirements change. The practices recommended here are designed to help server administrators with server security configuration. Server administrators managing various existing UDSM servers, should confirm that their servers conform to the established UDSM's security requirements.
- It is worth noting that security configuration guides and checklists for many OSs are publicly available, hence they may also be consulted to complement what has been presented in this document. Some automated tools also exist for securing OSs, and their use is recommended where applicable.

Guidelines

After planning the installation and deployment of the OS, as described in Section 4.4.6, and installing it, the following basic steps are necessary to secure the OS:

i. Patch and Upgrade Operating System- all applied patches or upgrades must be installed to correct known vulnerabilities.

ii. Any known vulnerabilities that an OS has, should be corrected before using it to host a server because it may expose it to untrusted users. To adequately detect and correct these vulnerabilities, server administrators should do the following:

   a. *Create, document and implement a patching process.*
   b. *Identify vulnerabilities and applicable patches.*
   c. *Mitigate vulnerabilities temporarily if needed and if feasible (until patches are available, tested and installed).*
   d. *Install permanent fixes (patches, upgrades, etc.)*

iii. Administrators should ensure that servers are adequately protected during the patching process.

iv. When preparing new servers for deployment, administrators should do either of the following:

   a. *Keep the servers disconnected from networks or connect them only to an isolated "build" network until all patches have been transferred to the servers through other means (e.g., removable storage devices) and installed. Then the other configuration steps listed in this section have been performed.*
   b. *Place the servers on a virtual local area network (VLAN) or other network segment that severely restricts what actions the hosts on it can perform and what communications can reach the hosts—only allowing those events that are necessary for patching and configuring the hosts. Do not transfer the hosts to regular network segments until all the configuration steps listed in this section have been performed.*
   c. *Administrators should generally not apply patches to production servers without first testing them on another identically configured server because patches can*

inadvertently cause unexpected problems with proper server operation. Although administrators can configure servers to download patches automatically, the servers should not be configured to install them automatically so that they can first be tested.

v. Hardening and Securely Configuring the OS - Administrators should perform the following steps to harden and securely configure a server OS so as to address security adequately:

   a. Server operating systems should be configured to operate only those services required to fulfil the operational requirements of the system.

   b. All unnecessary Services, Applications and Network Protocols should be removed or disabled. Ideally, a server should be on a dedicated, single-purpose host. If possible, install the minimal OS configuration and then add, remove, or disable services, applications and network protocols as needed.

   c. Completely remove unnecessary services and applications to simply disabling them through configuration settings. Attacks that attempt to alter settings and activate a disabled service cannot succeed when the functional components are completely removed. Disabled services could also be enabled inadvertently through human error.

   d. Systems must be initially hardened before they are deployed and must be regularly monitored.

   e. Administrators should consider configuring the OS to act as a bastion host for high security situations. The details of establishing a bastion host are necessarily OS-specific, so they are outside the scope of this SOP.

   f. Configure server resource controls appropriately.

vi. DoICT should determine the services to be enabled on a server. Additional services that might be installed include web servers, database access protocols, file transfer protocols and remote administration services. These services may be required in certain instances, but they may increase the risks to the server. The rule of thumb is that where the risks outweigh the benefits of having a service enabled, the decision shall be to disable or remove the service.

vii. If a remote control or remote access program is absolutely required and it does not strongly encrypt its communications, it should be tunnelled over a protocol that provides encryption, such as secure shell (SSH) or Internet Protocol Security (IPsec).

viii. Configure OS User Authentication - For servers, the authorized users who can configure the OS are limited to a small number of designated server administrators. The users who can access the server, however, may range from a few authorized employees to the entire Internet community. To enforce policy restrictions, if required, the server administrator should configure the OS to authenticate a prospective user by requiring proof that the user is authorized for such access. Even if a server allows unauthenticated access to most of its services, administrative and other types of specialized access should be limited to specific individuals and groups.

ix. In special situations, such as where high-value or high-risk servers are involved, use of authentication hardware, such as tokens or one-time password devices is recommended.

x. Use of authentication mechanisms where authentication information is reusable (e.g., passwords) and transmitted over an untrusted network, is strongly discouraged because the information can be intercepted and used by an attacker to masquerade as an authorized user.

xi. To ensure that the appropriate user authentication is in place, the following steps are recommended:

   a. *Remove or Disable Unneeded Default Accounts—The default configuration of the OS often includes guest accounts (with and without passwords), administrator or root level accounts, and accounts associated with local and network services.*

   b. *Disable Non-Interactive Accounts: accounts and the associated passwords that need to exist but do not require an interactive login. For Unix systems, disable the login shell or provide a login shell with NULL functionality (e.g., /bin/false).*

   c. *Create the User Groups—Assign users to the appropriate groups. Then assign rights to the groups, as documented in the deployment plan.*

   d. *Create the User Accounts—the deployment plan identifies who will be authorized to use each computer and its services. Create only the necessary accounts and permit the use of shared accounts only when no viable alternatives exist. Have ordinary user accounts for server administrators that are also users of the server.*

   e. *Configure Automated Time Synchronization—Some authentication protocols, such as Kerberos, will not function if the time differential between the client host and the authenticating server is significant. Therefore, servers using such protocols should be configured to automatically synchronize system time with a reliable time server. Typically, the time server is internal to the organization and uses the Network Time Protocol (NTP) for synchronization; publicly available NTP servers are also available on the Internet.*

   f. *Check the UDSM's Password guideline—Set account passwords appropriately. Elements that may be addressed in a password guideline include the following:*

      - *Length—a minimum length for passwords.*
      - *Complexity—the mix of characters required. An example is requiring passwords to contain uppercase letters, lowercase letters, nonalphabetic characters and to not contain "dictionary" words.*
      - *Aging—how long a password may remain unchanged.*
      - *Reuse—whether a password may be reused. Some users may try to defeat a password aging requirement by changing the password to one they have used previously.*

- *Authority—who is allowed to change or reset passwords and what sort of proof is required before initiating any changes.*
- *Password Security—how passwords should be secured, such as not storing passwords unencrypted on the server, and requiring administrators to use different passwords for their server administration accounts than their other administration accounts.*
- *Configure Computers to Prevent Password Guessing—It is relatively easy for an unauthorized user to try to gain access to a computer by using automated software tools that attempt all passwords. If the OS provides the capability, configure it to increase the period between login attempts with each unsuccessful attempt. If that is not possible, the alternative is to deny login after a limited number of failed attempts (e.g., three). Typically, the account is "locked out" for a period of time (such as 30 minutes) or until a user with appropriate authority reactivates it.*
- *Install and configure other Security Mechanisms to strengthen authentication—If the information on the server requires it, consider using other authentication mechanisms such as biometrics, smart cards, client/server certificates, or one-time password systems.*
- *Since, attackers using network sniffers can easily capture passwords passed across a network in clear text. Passwords must properly be protected while in transit. Authentication and encryption technologies, such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Shell (SSH), or virtual private networks using IPsec or SSL/TLS, must be implemented to protect passwords during transmission over untrusted networks.*

xii. Configure Resource Controls Appropriately - specify access privileges for individual files, directories, devices and other computational resources. By carefully setting access controls and denying personnel unauthorized access, the server administrator can reduce intentional and unintentional security breaches. For example, denying read access to files and directories helps to protect confidentiality of information, and denying unnecessary write (modify) access can help maintain the integrity of information. Limiting the execution privilege of most system-related tools to authorized system administrators can prevent users from making configuration changes that could reduce security. It also can restrict the attacker's ability to use those tools to attack the server or other hosts on the network.

xiii. Enable auditing to monitor attempts to access protected resources.

xiv. Configure the OS so as to provide an isolated virtual environment that the server software will be run within. The OS is configured so that server processes and user actions cannot "break out" of the environment.

4.4.11. Install and Configure Additional Security Controls

Often OSs do not include all security controls necessary to adequately secure it, its services, and applications. In such cases, administrators need to select, install, configure, and maintain additional software to provide the missing controls. To add the commonly needed security controls, observe the following guidelines:

Guidelines

i. Use anti-malware software, such as antivirus software, anti-spyware software and rootkit detectors, to protect the local OS from malware and to detect and eradicate any infections that occur. Anti-malware software is helpful when an infected media is connected to the server and a network service worm contacts the server.

ii. Use host-based intrusion detection and prevention software (IDPS) (such as file integrity checking software that can identify changes to critical system files) to detect attacks performed against the server, including DoS attacks.

iii. Use host-based firewalls, to protect the server from unauthorized access.

iv. Use patch management or vulnerability management software to ensure that vulnerabilities are addressed promptly. Such software solutions can be used only to apply patches or identify new vulnerabilities in the server's OSs, services and applications.

v. Use disk encryption technologies (if applicable to the server) to protect its stored data from attackers who may gain physical access to the servers. Disk encryption technologies may be in-built to operating systems or as third-party disk encryption products.

vi. When planning for security controls, consider the resources that security controls will consume to avoid degrading server's performance if it does not have enough memory and processing capacity.

vii. Consider any other network-based security controls, such as network firewalls and intrusion detection systems that could provide additional protection for the server.

viii. If host-based security controls are too resource-intensive for a server or are otherwise infeasible, compensate by using additional network-based security controls to protect the server's OS, services and applications. The normal practice is to use network-based security controls in addition to host-based security controls to provide additional layers of security.

4.4.12. Security Testing the Operating System

Periodic security testing of the OS is a vital way to identify vulnerabilities and to ensure that existing security precautions are effective and that security controls are configured properly. Common methods for testing OSs include vulnerability scanning and penetration testing.

- Vulnerability scanning usually entails using an automated vulnerability scanner to scan a host or group of hosts on a network for application, network and OS vulnerabilities.
- Penetration testing is a testing process designed to compromise a network using the tools and methodologies of an attacker. It involves iteratively identifying and exploiting the

weakest areas of the network to gain access, eventually compromising the overall security of the network.

Guidelines

i. Vulnerability scanning should be conducted to validate that OSs and server software are up-to-date on security patches and software versions. Also, it is recommended to run a vulnerability scan whenever a new vulnerability database is released for the scanners application which UDSM uses.

ii. Vulnerability scanning should be conducted periodically to all applicable UDSM servers, at least weekly to monthly, and penetration testing at least once annually.

iii. Before running any scanner, server should be installed with the latest updates to its vulnerability database. Some databases are updated more regularly than others, hence the frequency of updates should be a major consideration when choosing a vulnerability scanner.

iv. Because of the potential negative impact of vulnerability scanning, administrators may wish to scan 'test servers' first with new vulnerability database updates to ascertain their impact on the servers before scanning the production servers.

v. Vulnerability scanning results should be documented and deficiencies that may be discovered should be immediately corrected.

vi. Sever administrators should also consider running more than one vulnerability scanner, since no scanner is able to detect all known vulnerabilities. A recommended practice here, is to use one commercial and one freeware scanner. A combination of network-based and host-based vulnerability scanners may also be considered.

vii. Vulnerability scanners should be used to provide the following capabilities:

   a. Identifying active hosts on a network.

   b. Identifying active services (ports) on hosts and which of these are vulnerable.

   c. Identifying applications and banner grabbing.

   d. Identifying Oss.

   e. Identifying vulnerabilities associated with discovered OSs, server software and other applications.

   f. Testing compliance with or deviations from the UDSM's ICT security policy.

viii. Utmost care must be observed when penetrating testing has to be done as it is a very labour-intensive activity and requires great expertise to minimize the risk to targeted systems. It may slow the network response time because of network mapping and vulnerability scanning and systems may be damaged or rendered inoperable in the course of penetration testing.

ix. Penetration testing tools should be used to achieve the following:

a. *To test the network using the same methodologies and tools employed by attackers.*

b. *To verifies whether vulnerabilities exist.*

c. *To go beyond surface vulnerabilities and demonstrates how these vulnerabilities can actually be exploited iteratively to gain greater access.*

d. *To demonstrates that vulnerabilities are not purely theoretical.*

e. *To create the "realism" necessary to address security issues.*

f. *To test procedures and susceptibility of the human element to social engineering.*

x. Security Testing should preferably be conducted on non-production servers. Factors to be considered when deciding whether to test the production server or a similarly configured non-production server include the following:

a. *The possible impact to the production server: For example, if a certain test technique is likely to cause a denial of service, then that technique should probably be used against the non-production server.*

b. *The presence of sensitive information: If testing could expose this information to people without authorization, then the testing should be performed on a non-production server that holds a false (dummy) version of the original information.*

c. *Configuration similarity of production and non-production servers: in practice, there are usually inconsistencies between the test and production environments, which can result in missed vulnerabilities if the non-production servers are used.*

4.4.13. Securing the Server Software

Once the OS has been installed and secured, as described in preceding sections, the next step is to install and secure the chosen server software (e.g. SQL server).

Guidelines

i. Before starting this process, read the server software documentation carefully and understand various options available for the installation process. Visit the server software manufacturer's website or vulnerability database to determine whether there are known vulnerabilities and related patches available that should be installed or configured as part of the setup process. Useful websites include:

a. *Security Vulnerability Database (CVE) at https://www.cvedetails.com*

b. *National Vulnerability Database (NVD), at https://nvd.nist.gov*

c. *VulDB at https://vuldb.com*

Only after these preliminary steps are accomplished should the installation start. Note that specific directions for particular servers are available from server manufacturers and from security checklist repositories.

ii. A partially configured and/or patched server should not be exposed to external networks or users to avoid unforeseen compromise. Similarly, internal network access should be as limited as possible until all software packages are installed, patched and securely configured.

iii. The platform has to be hardened before placing it on the network. However, such practice is not always feasible because some application packages and tool combinations cannot be installed, configured and tested on top of a pre-hardened OS and Web server configuration. In such situations, stepwise or incremental hardening is a viable option to consider, with full validation of complete hardening occurring at production deployment.

4.4.14. Securely Installing the Server Software

In many respects, the secure installation and configuration of the server software mirrors the OS process discussed earlier. The overarching principle, as before, is to install only the services required for the server and to eliminate any known vulnerabilities through patches or upgrades. Any unnecessary applications, services, or scripts that are installed should be removed immediately once the installation process is complete. During the installation of the server software, the following guidelines should be observed.

Guidelines

i. Install the server software either on a dedicated host or on a dedicated guest OS if virtualization is being employed.

ii. Apply any patches or upgrades to correct for known vulnerabilities in the server software.

iii. Create a dedicated physical disk or logical partition (separate from OS and server application) for server data, if applicable.

iv. Remove or disable all services installed by the server application but not required (e.g., gopher, FTP, HTTP, remote administration).

v. Remove or disable all unneeded default user accounts created by the server installation.

vi. Remove all manufacturers' documentation from the server.

vii. Remove all example or test files from the server, including sample content, scripts and executable code.

viii. Remove all unneeded compilers.

ix. Apply the appropriate security template or hardening script to the server.

x. For external-facing servers, reconfigure service banners not to report the server and OS type and version, if possible.

xi. Configure warning banners for all services that support such banners.

xii. Configure each network service to listen for client connections on only the necessary TCP and UDP ports, if possible.

xiii. As a security measure, it is advisable to install the server with non-standard directory names, directory locations and filenames if possible. Experience shows that many server attack tools and worms targeting servers only look for files and directories in their default locations. While this will not stop determined attackers, it will force them to work harder to compromise the server, and it also increases the likelihood of attack detection because of the failed attempts to access the default filenames and directories and the additional time needed to perform an attack.

4.4.15. Configuring Access Controls

- Most server OSs provide the capability to specify access privileges individually for files, devices and other computational resources. Any information that the server can access using configuration access controls can potentially be distributed to all users accessing it. The server software is likely to include mechanisms to provide additional file, device and resource access controls specific to its operation. Additionally, many servers support a range of technologies for identifying and authenticating users with differing privileges to access information.

- Encryption can be used to protect information traversing the connection between a server and a client. Without encryption, anyone with access to the network traffic can determine, and possibly alter, the content of sensitive information, even if the user accessing the information has been authenticated. This may violate the confidentiality and integrity of critical information.

- The proper setting of access controls can help prevent the disclosure of sensitive or restricted information that is not intended for public dissemination. In addition, access controls can be used to limit resource use in the event of a DoS attack against the server. Similarly, they can enforce separation of duty by ensuring server logs cannot be modified by server administrators and potentially ensure that only the server process is allowed to append to the log files.

Guidelines

i. It is recommended to set identical permissions for both the OS and server application, otherwise, too much or too little access may be granted to users.

ii. Server administrators should consider how best to configure access controls to protect information stored on servers from two perspectives:

a. To limit the access of the server application to a subset of computational resources.

b. To limit the access of users through additional access controls enforced by the server, where more detailed levels of access control are required.

iii. Typical files to which access should always be controlled are as follows:

a. Application software and configuration files

   b. *Files related directly to security mechanisms*
   c. *Password hash files and other files used in authentication*
   d. *Files containing authorization information used in controlling access*
   e. *Cryptographic key material used in confidentiality, integrity and non-repudiation services*
   f. *Server log and system audit files*
   g. *System software and configuration files*
   h. *Server content files.*

iv. Stronger cryptographic technologies must always be used for implementing authentication and encryption technologies for UDSM's servers *(e.g., Symmetric Key Cryptography - include AES, 3DES and Blowfish; Asymmetric Key Cryptography - include RSA and Elliptic Curve Cryptography; Hashing - SHA-256 and SHA-512; Digital Signatures - include RSA and DSA).*

v. When weaknesses are identified in existing cryptographic technologies, DoICT should prepare a plan and facilitate a migration of the servers to stronger cryptographic technologies; and should always stay aware of cryptographic requirements and recommendations and plan to update the servers accordingly.

vi. The server application should only execute under a unique individual user and group identity with very restrictive access controls.

vii. New user and group identities should be established for exclusive use by the server software.

viii. The new user and new group should be independent from all other users and groups and unique. This is a prerequisite for implementing access controls described in the following steps.

   a. *During initialization, the server may have to run with root (Unix) or administrator/system (Windows) privileges;*
   b. *ensure that the server is configured to reduce its privileges to those of the server user after performing its initialization functions.*

ix. Use the server OS to further limit which files can be accessed by the service processes. These processes should have read-only access to those files necessary to perform the service and should have no access to other files, such as server log files.

x. Use server host OS access controls to enforce the following:

   a. *Service processes are configured to run as a user with a strictly limited set of privileges (i.e., not running as root, administrator, or equivalent).*
   b. *Service processes can only write to server content files and directories if necessary.*

c. *Temporary files created by the server software are restricted to a specified and appropriately protected subdirectory (if possible). Access to these temporary files is limited to the server processes that created the files (if possible).*

xi. Ensure that the server software cannot save (or, in some cases, read) files outside the specified file structure dedicated to server content. This may be a configuration choice in the server software, or it may be a choice in how the server process is controlled by the OS. Ensure that such directories and files (outside the specified directory tree) cannot be accessed both directly and through the server software.

4.4.16. Server Resource Constraints

To mitigate the effects of certain types of DoS attacks, configure the server in such a way to limit the amount of OS resources it can consume. Doing so protects it against attacks that attempt to fill the file system on the server OS with extraneous and incorrect information that may cause the server to crash. Logging information generated by the server OS may help in recognizing such attacks. Where applicable observe the following guidelines.

Guidelines

i. Server content should be installed on hard drive or logical partition different from the one with the OS and server software *(e.g., partitions for OS, database server [DBMS] and then the database itself).*

ii. A limit should be placed on the amount of hard drive space that is dedicated for uploads, if uploads to the server are allowed. Ideally, uploads should be placed on a separate partition to provide stronger assurance that the hard drive limit cannot be exceeded.

iii. If uploads are allowed to the server, ensure that these files are not readable by the server until after some automated or manual review process is used to screen them. This measure prevents the server from being used to propagate malware or traffic pirated software, attack tools, pornography, etc.

iv. It is also recommended to limit the size of each uploaded file, which could limit the potential effects of a DoS attack involving uploading many large files.

v. Ensure that log files are stored in a location that is sized appropriately. Ideally, log files should be stored on a separate partition. If an attack causes the size of the log files to increase beyond acceptable limits, a physical partition helps to ensure the server has enough resources to handle the situation appropriately.

vi. Configure the maximum number of server processes and/or network connections that the server should allow.

vii. Server logs should be stored on centralized logging servers whenever possible and also locally in the server itself if feasible. If an attack causes the server to be compromised, the attacker could modify or erase locally stored logs to conceal information on the attack. Hence, maintaining a copy of the logs on a centralized logging server gives administrators more information to use when investigating such a compromise.

viii. To further reduce the impact of certain DoS attacks, it is often necessary to configure timeouts and other controls. One type of DoS attack takes advantage of the practical limits on simultaneous network connections by quickly establishing connections up to the maximum permitted, such that no new legitimate users can gain access. By setting network connection timeouts (the time after which an inactive connection is dropped) to a minimum acceptable time limit, established connections will time out as quickly as possible, opening new connections to legitimate users. This measure only mitigates the effects; it does not defeat the attack.

ix. If the maximum number of open connections (or connections that are half-open) is set to a low number, an attacker can easily consume the available connections with illegitimate requests (often called a SYN flood). Setting the maximum to a much higher number may mitigate the effect of such an attack, but at the expense of consuming additional resources. Note that this is only an issue for servers that are not protected by a firewall that stops SYN flood attacks. Most enterprise-level firewalls protect servers from SYN floods by intercepting them before they reach the servers.

4.5. Maintaining the Security of the Server

After initially deploying a server, administrators need to maintain its security continuously. Vital activities in several administration include handling and analysing log files, performing regular server backups, recovering from server compromises (if any), testing server security regularly and performing remote administration securely. As presented in earlier section, security configuration guides and checklists are publicly available for many OSs and server software; many of these documents contain OS and server-specific recommendations for security maintenance. Other maintenance activities presented in earlier sections, and thus not duplicated here, include testing and deploying OS and server patches and updates, maintaining the secure configuration of the OS and server software, and maintaining additional security controls used for the server.

4.5.1. Logging and Handling of Log Files

Logging is a cornerstone of a sound security posture. Capturing the correct data in the logs and then monitoring those logs closely is vital. Network and system logs are important, especially system logs in the case of encrypted communications, where network monitoring is less effective. Server software can provide additional log data relevant to server-specific events.

Guidelines

i. Log files are often the only record of suspicious behaviour which can be reviewed after the fact, hence mechanisms for information logging must be enabled and monitored. This allows the logs to be used to detect failed and successful intrusion attempts and to initiate alert mechanisms when further investigation is needed. Among others, server logs may provide:

a. *Alerts to suspicious activities that require further investigation*
b. *Tracking of an attacker's activities*
c. *Assistance in the recovery of the server*
d. *Assistance in post-event investigation*
e. *Required information for legal proceedings*

ii. DICT should ensure that specific procedures and tools for each type of server used at UDSM are in place to process and analyse the log files and to review alert notifications.

iii. The selection and implementation of specific server software will determine which actions the server administrator should perform to establish logging configurations. Since, each type of server software supports different logging capabilities. For example, some server software may use a single log, while other server software may use multiple logs (each for different types of records); some server software permits administrators to select from multiple log formats, such as proprietary, database and delimiter-separated, etc.

iv. If a server supports the execution of programs, scripts, or plug-ins, it may be necessary for the programs, scripts, or plug-ins to perform additional logging. Often, critical events take place within the application code itself and will not be logged by the server.

v. If server administrators develop or acquire application programs, scripts, or plug-ins, it is strongly recommended that they define and implement a comprehensive and easy-to-understand logging approach based on the logging mechanisms provided by the server host OS. Log information associated with programs, scripts and plug-ins can add significantly to the typical information logged by the server and may prove invaluable when investigating events.

vi. Server administrators must ensure that sufficient log capacity is available, because logs often take considerably more space than administrators may initially estimate, especially when logging is set to a highly detailed level.

vii. Server administrators should closely monitor the size of the log files when they implement different log settings to ensure that the log files do not fill up the allocated storage.

viii. In a situation where the size of the log files grows rapidly, removing and archiving the logs more frequently or reducing the logging level of detail may be necessary.

ix. Some server programs provide a capability to enforce or disable the checking of specified access controls during program startup. This level of control may be helpful, for example, to avoid inadvertent alteration of log files because of errors in file access administration. Hence server administrators should determine the circumstances under which they may wish to enable such checks (assuming the server software supports this feature).

x. All UDSM servers should use time synchronization technologies, such as the Network Time Protocol (NTP), to keep their internal clocks synchronized with an accurate time source. This provides accurate timestamps for logs.

4.5.2. Reviewing and Retaining Log Files

Reviewing log files is a tedious and time-consuming task that informs administrators of events that have already occurred. Accordingly, files are often useful for corroborating other evidence, such as a CPU utilization spike or anomalous network traffic reported by an IDPS. When a log is used to corroborate other evidence, a focused review is in order. For example, if an IDPS reported a suspicious outbound FTP connection from a Web server at 8:17 a.m., then a review of the logs generated around 8:17 a.m. is appropriate.

Guidelines

i. Server logs should always be reviewed for indications of attacks.

ii. The frequency of the reviews should be based on the following factors:

   a. Amount of traffic the server receives

   b. General threat level (e.g. certain servers may receive many more attacks than other servers and thus should have their logs reviewed more frequently)

   c. Emergence of specific threats (at certain times, specific threats arise that may require more frequent log file analysis)

   d. Vulnerability of the server

   e. Value of data and services provided by the server.

iii. Generally, reviews should take place regularly (e.g., daily) and when a suspicious activity has been noted or a threat warning has been issued.

iv. The review task could quickly become burdensome to a server administrator since servers receive significant amounts of traffic, and the log files may quickly become voluminous. Hence to reduce this burden, automated log analysis tools should be installed to ease the burden on server administrators.

v. The automated log analyser should forward any suspicious events to the responsible server administrator or security incident response team as soon as possible for follow-up investigation.

vi. If situation calls for it, administrators may use two or more log analysers, which will reduce the risk of missing an attacker or other significant events in the log files when a single analyser is used.

vii. A long-term and more in-depth analysis of the logs is needed. Because a server attack can involve hundreds of unique requests, an attacker may attempt to disguise a server attack by increasing the interval between requests. In this case, reviewing daily or weekly logs may not show recognizable trends. However, when trends are analysed over a week, month, or quarter, multiple attacks from the same host or subnet can be more easily recognized.

viii. Log files should be protected to ensure that if an attacker does compromise a server, the log files cannot be altered to cover the attack. Although encryption can be useful in protecting log files, the best solution is to store log files on a host separate from the server. This is often called a centralized logging server.

ix. Centralized logging is often performed using syslog, which is a standard logging protocol. Alternately, administrators can use Security Information and Event management (SIEM) software that uses centralized servers to perform log analysis, database servers to store logs, and either agents installed on the individual hosts or processes running on the centralized servers to transfer server logs or log data from the hosts to the servers and parse the logs.

x. Log files should be backed up and archived regularly. Archiving log files for a period of time is important for several reasons, including supporting certain legal actions and troubleshooting problems with the server. The retention period for archived log files depends on a number of factors, including the following:

   a. *Legal and regulatory requirements*
   b. *Institutional requirements and relevant policies*
   c. *Size of logs (which is directly related to the traffic of the site and the number of details logged)*
   d. *Value of server data and services*
   e. *Threat level.*

4.6. Server Backup

One of the most important functions of a server administrator is to maintain the integrity of the data on the server. This is important because servers are often some of the most exposed and vital hosts on any organization’s network. The server administrator needs to perform backups of the server on a regular basis for several reasons. A server could fail as a result of a malicious or unintentional act or a hardware or software failure. In addition, Server data should also be backed up regularly for legal and financial reasons.

4.6.1. Server Backup Types and Standards

Three primary types of backups exist: **full, incremental and differential**. Full backups include the OS, applications and data stored on the server (i.e., an image of every piece of data stored on the server hard drives). The advantage of a full backup is that it is easy to restore the entire server to the state (e.g., configuration, patch level, data) it was in when the backup was performed. The disadvantage of full backups is that they take considerable time and resources to perform. Incremental backups reduce the impact of backups by backing up only data that has changed since the previous backup (either full or incremental).

Differential backups reduce the number of backup sets that must be accessed to restore a configuration by backing up all changed data since the last full backup. However, each differential backup increases as time lapses from the last full backup, requiring more processing time and storage than would an incremental backup need. Generally, full backups are performed less frequently (weekly to monthly or when a significant change occurs), and incremental or differential backups are performed more frequently (daily to weekly). The frequency of backups will be determined by several factors; hence the following factors should be considered as guidelines:

Guidelines

i. For static content such as a relatively static web pages, less frequent backups should be done.

ii. For dynamic content such as financial transactions, more frequent backups should be done.

iii. Generally, server backup must always be done; the nature of the backups will be determined by the following factors, among others:

   a. *Volatility of information on the server/site*
   b. *Volatility of configuring the server*
   c. *Type of data to be backed up (e.g., system, application, log, or user data)*
   d. *Amount of data to be backed up*
   e. *Backup device and media available for the purpose*
   f. *Time available for dumping backup data*
   g. *Criticality of data*
   h. *Threat level faced by the server*
   i. *Effort required for data reconstruction without data backup*
   j. *Other data backup or redundancy features of the server (e.g., if the server has Redundant Array of Inexpensive Disks [RAID]).*

iv. Where possible, maintain a Test Server with hardware and software identical to the production or live server and be located on an internal network segment (intranet) where it can be fully protected by the perimeter network defences installed at the University. Having a test server offers numerous advantages:

   a. *It provides a platform to test new patches and service packs before application on the production server.*

b. *It provides a development platform for the server administrator to develop and test new content and applications.*

c. *It provides a platform to test configuration settings before applying them to production servers.*

d. *Software critical for development and testing but that might represent an unacceptable security risk on the production server can be installed on the development server (e.g., software compliers, administrative tool kits, remote access software).*

4.6.2. Recovering From a Security Compromise

At some point we assume that eventually UDSM will face a successful compromise of one or more hosts on its network. Hence it is important to create and document the required procedures for responding to successful intrusions. The response procedures outline the actions that are required to respond to a successful compromise of the server and the appropriate sequence of these actions (sequence can be critical). The guidelines listed in this subsection presume existence of a dedicated incident response team (among the technical staff) within DICT, that is contacted immediately when there is suspicion or confirmation of a compromise of the University network.

Guidelines

i. A server administrator should be aware of the relevant UDSM's policies and procedures for incident handling, and follow them accordingly

ii. The server administrator should immediately contact the designated incident response team within DICT for guidance before any action is taken after a suspected or confirmed security compromise.

iii. The following are recommended steps to be performed after discovering a successful compromise:

   a. *Server administrators report the incident to the designated computer incident response team within the DICT*

   b. *Server administrator and the team isolate the compromised systems or take other steps to contain the attack so that additional information can be collected. One method to isolate a server would be to reconfigure the nearest upstream switch or router.*

   c. *DoICT and the team consult expeditiously, as appropriate, with UDSM Management. Based on the severity of the incident, the management may contact law enforcement organs and other external organs such as TZ-CERT.*

   d. *If legal action is to be pursued, server administrators and the team need to be aware of the guidelines for handling a host after a compromise. They can consult UDSM legal unit and relevant law enforcement authorities as appropriate.*

e. Server administrator and the team should investigate similar hosts within UDSM to determine if the attacker also has compromised other systems.

f. *Server administrator and the team should analyse the intrusion, including*:

- *Establishing the current state of the affected server, starting with the most short-lived data (e.g., current network connections, memory dump, files time stamps, logged in users, etc.)*
- *Whether there are modifications made to the server's software and configuration*
- *Whether there are modifications made to the data*
- *Whether there are tools or data left behind by the attacker*
- *System, intrusion detection and firewall log files.*

g. Server administrator and the team should restore the server before redeploying it. This can be done by either install a clean version of the OS, applications, necessary patches and server content; or restore the server from backups (this option can be riskier because the backups may have been made after the compromise, and restoring from a compromised backup may still allow the attacker access to the server).

h. The decision whether to reinstall the OS of a compromised server or restore it from a backup shall be made after considering several factors. Factors that should considered include the following among others:

- *Level of access that the attacker gained (e.g., root, user, guest, system)*
- *Type of attacker (internal or external)*
- *Purpose of compromise (e.g., Web page defacement, illegal software repository, platform for other attacks, data exfiltration)*
- *Method used for the server compromise*
- *Actions of the attacker during and after the compromise (e.g., log files, intrusion detection reports)*
- *Duration of the compromise*
- *Extent of the compromise on the network (e.g., the number of hosts compromised)*
- *Results of consultation with management and legal counsel.*

i. The lower the level of access gained by the intruder and the more the server administrator and the team understand about the attacker's actions, the less risk there is in restoring from a backup and patching the vulnerability.

j. For incidents in which there is less known about the attacker's actions and/or in which the attacker gains high-level access, it is recommended that the OS, server software and other applications be reinstalled from the manufacturer's original *distribution media and that the server data be restored only from a known good backup.*

k. *After the server has been restored successfully, server administrator and the team should harden the server by disabling unnecessary services and applying all necessary patches.*

l. *All passwords (including on uncompromised hosts, if their passwords are believed to have been seen by the compromised server, or if the same passwords are used on other hosts) should be changed.*

m. *Then, reconfigure network security elements (e.g., firewall, router, IDPS) to provide additional protection and notification.*

n. *The restored server should undergo security test to ensure security.*

o. *Finally, server is reconnected to the network and should be continuously monitored for signs whether the attacker is attempting to access the server or network again.*

p. *After all the steps outlined above have been completed, the lessons learned from the compromise and containment should be documented*

4.6.3. Administering a Server Remotely

Remote administration of a server should be allowed only after careful consideration of the risks. The risk of enabling remote administration varies considerably depending on the location of the server on the network. For a server that is located behind a firewall, remote administration can be implemented relatively securely from the internal network, but not without added risk. Remote administration should generally not be allowed from a host located outside the University's network unless it is performed from an institutional-controlled computer through an approved University's remote access solution, such as a VPN. If it is inevitably necessary to remotely administer a server, the following guidelines may help to ensure that remote administration is implemented as securely as possible:

Guidelines

i. A strong authentication mechanism should be used (e.g., public/private key pair, two-factor authentication).

ii. Restrict which hosts can be used to remotely administer the server.

iii. Restrict by authorized users

iv. Restrict by IP address (not hostname)

v. Restrict to hosts on the internal network or those using the approved institutional enterprise-class remote access solution.

vi. Use secure protocols that can provide encryption of both passwords and data (e.g., SSH, HTTPS); do not use less secure protocols (e.g., telnet, FTP, NFS, HTTP) unless absolutely required and tunnelled over an encrypted protocol, such as SSH, SSL/TLS, or IPsec.

vii. Enforce the concept of least privilege on remote administration (e.g., attempt to minimize the access rights for the remote administration accounts).

viii. Do not allow remote administration from the Internet through the firewall unless accomplished via strong mechanisms, such as VPNs.

ix. Use remote administration protocols that support server authentication to prevent man-in-the-middle attacks.

x. Change any default accounts or passwords for the remote administration utility or application.

5. Network Security Management Guidelines

5.1. Application

The Network Security Management Standard applies to all the computing network laid down at UDSM (whether wired or wireless) and the associated devices and systems.

5.2. Purpose

To provide measures to prevent, detect and correct network compromises, and computer systems compromises through the UDSM network.

5.3. Scope

This guideline applies to all UDSM's network devices that connect to the centrally managed UDSM's network infrastructure (core, distribution and access networks) or that which process confidential or operationally critical information, whether such information is part of the UDSM's centrally managed infrastructure or not.

5.4. Network Security Management Requirements

This subsection outlines a set of requirements for an effective network security management at UDSM for which standard operation procedures are recommended. The requirements are on the following security issues and associated controls:

i. Physical Security
ii. Authentication
iii. Secure Network Management
iv. Intrusion Prevention and Detection System
v. Anti-Spoof Measures
vi. Change Control
vii. Logging and Monitoring
viii. Password Management
ix. Configuration Management
x. Virtual Private Network
xi. Vulnerability Scanning
xii. Wireless Security
xiii. Device Registration and
xiv. Network Devices

5.4.1. Physical Security Controls

Guidelines

i. All UDSM's network devices should be secured in an area with physical access control.
ii. Core network equipment should be located in an alarmed area monitored with CCTV cameras.

iii. Core network equipment should be attached to an appropriately designed UPS and generator system.

5.4.2. Authentication and Access Lists

Guidelines

i. Access to network devices should be controlled by access lists so that the equipment is accessible only from a limited number of locations.

ii. Access to configuration backups should be restricted to authorized personnel only.

iii. All networks should be protected from Layer-3 IP address spoofing by an access list or other means.

iv. All external connections to UDSM should be protected by an access list that blocks certain high-risk TCP/UDP ports.

v. This list shall be maintained by DICT and is reviewed by DICT on a yearly basis (or as needed). Changes are subject to the change control process.

vi. Centralized user-level authentication should be used to authenticate all interactive users making changes to all network devices.

vii. Hard-coded passwords will be allowed as necessary for non-interactive purposes, as well as recovery of devices that have become disconnected from the network.

viii. Whenever possible, network devices will display a trespassing banner at login.

ix. This banner text shall not provide the underlying characteristics of the network device (e.g. OS in use, or its version, etc.).

5.4.3. Network Management

Guidelines

i. Plain-text protocols should not be used in network management.

ii. Where possible, management traffic should be separated from user traffic.

iii. Network Device management interfaces should be on a designated management network.

iv. Any console ports used for device management should be secured by a username/password or other methods approved by the DICT.

v. Network management services should use secure protocols that do not use plaintext community strings.

vi. Default SNMP community strings should be changed.

vii. Outdated or vulnerable protocols should be prohibited (e.g. FTP, telnet, remote host protocols, SSHv1, SSLv1, SSLv2 and others).

5.4.4. Intrusion Detection and Prevention Systems (IDPS)

Guidelines

i. An IDPS service should be deployed on the links to/from the UDSM network and the public Internet. Hosts that are detected via the rule set of the deployed IDPS shall automatically be blocked from further network access until the cause of the detection is understood and remediated.

ii. The IDPS configuration will be reviewed by DICT every six months or upon changes to the configuration, or as situations warrant otherwise.

5.4.5. Anti ARP-Spoofing

Guidelines

i. Anti ARP-spoofing technologies should be deployed on user-edge Network Devices.

ii. Features that support DHCP/ARP snooping should be enabled on Network Devices to better secure layer-2 networks from techniques such as ARP spoofing.

5.4.6. Change Control

Guidelines

i. Any changes involving significant risk to the UDSM network should go through a change control process.

ii. The change control process should at least include:

   a. Problem statement

   b. Supporting data

   c. Potential solutions

   d. Impact/Risks

   e. Management approval of changes

5.4.7. Logging and Monitoring

Guidelines

i. All network devices should log to a designated logging/network management system.

ii. To ensure the integrity of the network, all network devices should be regularly monitored for their ability to be reached by the designated centralized network management system.

iii. Any logs, including but not limited to, network, telecom, security and IDPS logs shall be confidentially kept and protected.

5.4.8. Network Device Passwords

Guidelines

i. Passwords on network devices should be changed in accordance with the currently stated UDSM's password standard.

ii. All manufacturers' default passwords should be disabled or changed.

5.4.9. Network Configuration Backups

Guidelines

i. The configuration of all pieces of UDSM's network equipment should be backed up regularly.

ii. The configurations should be subject to managed revision control. Any changes in configuration should automatically and timely notify the network administrator(s).

iii. An audit of network configurations is recommended to be conducted by DICT from time to time.

5.4.10. Virtual Private Network (VPN)

Guidelines

i. Any VPN service that is deployed for use at UDSM should be configured to not allow connection to the Internet except through a designated UDSM gateway device.

ii. Any new VPN service should undergo a security review by DICT or any designated party appointed by DICT.

iii. Deployment of VPN at UDSM should observe and comply with applicable regulation as issued by the TCRA and other similar authorities, if any.

5.4.11. Vulnerability Scanning and Quarantine

Guidelines

i. The network should be scanned regularly for hosts that are vulnerable to remotely exploitable attacks. Hosts that are vulnerable will be "moved" to a quarantine network where they may be allowed to self-remediate or be attended to. Hence, DICT should ensure such a network is in place. The quarantine network will allow hosts to access services necessary to patch and remediate infections. These services may be provided through a proxy server.

ii. All data gathered from the vulnerability scanning and quarantine processes should be classified and treated as UDSM's confidential information.

iii. Notification to administrators of registered subnets or individual network addresses in the event of quarantine or blocking require the following:

   a. The local administrator of the registered UDSM subnet or individual addresses is responsible for maintaining accurate registration information.

b. *Unless the UDSM network may be harmed without immediate quarantine or blocking of compromised computers, the designated Network Administrator should notify administrators of systems found to be vulnerable by the vulnerability scanner before the systems are placed into quarantine or blocked.*

c. *If immediate quarantine or blocking is necessary to avoid harm to the UDSM network, the Network Administrator should notify the administrators of affected systems in a timely manner.*

5.4.12. Wireless Security

Guidelines

i. All new wireless Network Devices should support Encryption Methods which have been selected and approved by the DICT

ii. Minimum levels of security should be issued by the DICT and adhered to accordingly.

5.4.13. Device Registration

Guidelines

i. Before being allowed on the UDSM network, all network devices or systems with an IP address on the network should be registered in accordance with a registration procedure to be issued and approved by the DICT

ii. This device registration should include all MAC addresses and the name of the party responsible for the device.

iii. Guest access should be registered with appropriate contact information and duration of the provided access.

5.4.14. Purchase and Deployment of New Network Devices

Guidelines

i. All Network Devices purchased after the effective date of this standard should support all requirements of the standard.

ii. All Network Devices deployed after the effective date of this standard should be configured to implement all requirements of this standard.

5.4.15. Currently Deployed UDSM Network Devices

Guidelines

i. All UDSM's Network Devices currently deployed should comply with all requirements of the Standard.

ii. If an existing Network Device currently deployed at the UDSM's network is not capable of complying with a specific requirement of the Standards, then that specific requirement can be waived for that device after careful analysis and approval from the DICT office.