SNDT Women's University

Shreemati Nathibai Damodar Thackersey Women's University

Information Security Policies

Document Controls

Change Record

Distribution List

#	Name of the Custodian
1.	Registrar, SNDT Women’s University
2.	Information Security Committee
3.	Chief Information Security Officer
4.	Any other entity authorized by the Registrar

Contents

1. Introduction

This Document describes the Security Controls that should be implemented and practiced for various Information Assets, so as to ensure compliance to the Information Security Policies of Shreemati Nathibai Damodar Thackersey Women's University (hereinafter called as 'SNDTWU').

This document describes WHAT CONTROLS NEED TO BE IMPLMENTED.

• Structure of this document

This document is divided into various sections and each section is structured as under

- **Policy Objective:** This section describes the objective/s for which the policy has been defined.
- **Policy Scope**: This section defines various internal and external entities as well as the Information Assets to which that policy statement/s applies.
- **Policy Statements**: This section describes the Information Security Policies of SNDTWU for each control area.
- **Detailed Procedures**: This section describes the Information Security Procedures at detailed level, so as to comply with the Security Policy. However, this section does not describe the Technical and / or procedural details to implement these Procedures. These are described in the "third tier of documentation" i.e. The Security Implementation Guidelines / hardening guidelines.
- **Implementation Responsibilities**: This section describes the entities, who are responsible for the implementation of information security procedures for a given area.

NOTES:

There are certain policies and procedures in this document, the contents wherein are commonly applicable to various other policies and procedures. For e.g. password policy would be applicable to various other policies like O.S., databases, applications, etc. To avoid repetition and streamline the process of maintaining the policy all such "COMMON" policies have been defined separately and are referred where they are applicable.

Various operational formats which are applicable to the policies have not been included in this document. Since change / modification to such formats is purely an operational matter, such changes / modifications can be approved by the operational managers.

2. Asset Management Policy

Policy Objective

Objective of this policy is to define controls for management of assets owned by SNDTWU. These guidelines are defined to ensure streamlining of asset procurement, maintenance and disposal. Inappropriate procurement / installation expose SNDTWU to various risks including virus attacks, compromise of network systems and services, licensing and other legal issues.

Policy Scope

This policy covers procurement of IT assets including Hardware, Software, and Services like ISP, Maintenance, etc. and is applicable to all concerned users of SNDTWU.

Policy Statements

1. All the IT Assets and Services shall be procured as per approved procedures in effect.
2. An up-to-date information asset register would be maintained.
3. All information assets shall be tagged / labelled appropriately.
4. Proper utilization of IT Assets and Services shall be ensured.
5. All the IT Assets shall be properly maintained and appropriate records of IT Services shall be kept up-to-date.
6. Proper security of IT Assets shall be ensured.
7. Movement of IT Assets shall be properly tracked and up-to-date records shall be maintained.
8. IT Assets shall be disposed off in secure manner.

3. Acceptable Usage Policy

Policy Objective

Objective of this policy is to outline the acceptable use of computer equipment and information assets at SNDTWU. These rules are in place to protect the users and SNDTWU. Inappropriate use exposes SNDTWU to risks including virus attacks, compromise of network systems and services and legal issues.

Policy Scope

This policy covers all information assets and all users of SNDTWU.

Policy Statements

1. Information assets shall be used for official purpose only
2. Every computer user shall know, understand and adhere to the Information Security Policies and Procedures
3. Users may use information assets for a limited personal usage prudently and ensure that it does not produce hindrance to the functionality or is not conflicting with SNDTWU’s policies (Responsible)
4. Users shall not add, modify or remove any system hardware and / or software component on the IT system provided by SNDTWU
5. Compliance to this policy is mandatory
6. Users shall take reasonable measures to protect the equipment from damage, theft or loss

4. Application Security Policy

Policy Objective

The Application Security Policy is designed to ensure that

- Application should meet the business and user requirements.
- Application should comply with various security requirements like authentication, authorisation and auditing controls.
- The Application should help ensure non-repudiation of any activities done by the users.
- Adequate controls are built into the Application software to prevent loss, modification or misuse of data.
- Changes to the Application systems are controlled and are done as per the change management policy.
- Application generates adequate and secure audit trails to help establish accountability.

Policy Scope

This policy is applicable to all Applications installed and used within SNDTWU and is applicable to all users including the employees, contractors, consultants and temporary users.

Policy Statements

1. The administration of each Application shall be identified and the roles and responsibilities shall be defined, documented and communicated
2. Up-to-date Inventory of the Applications shall be maintained
3. Application owners shall ensure safe custody of installation kits for applications owned by them
4. Only those components in applications which are necessary for the business shall be installed
5. Appropriate procedures shall be established for ensuring integrity of the systems
6. Appropriate Input, Process and Output controls shall be defined, designed, developed, implemented and tested
7. Controls over interfaces and intermediate Files shall be established
8. Applications accessible over internet shall be duly secured
9. Maker – Checker Controls over Inputs shall be established
10. Each application shall be tested for business functionality and security before being moved into production environment
11. Scripts which are developed outside of the Application for additional functionality shall be tested, documented and integrity control maintained

12. Appropriate procedures shall be established for User and Authorisation Management Controls

13. Appropriate procedures shall be established for Password Controls

14. Appropriate procedures shall be established for Log Management Controls

15. Appropriate procedures shall be established for Backup Management Controls

5. Web Server Security Policy

Policy Objective

- To ensure that the web servers (intranet and internet facing) are configured for security as per the business, Applications and Security requirements
- Various services made available to the users are controlled and are as per the business, Application and Security requirements
- Traffic to and from the web servers is secured as per the business and Application requirements.

Policy Scope

This policy is applicable to all web servers and various services that may be made accessible to the users over intranet and internet.

Policy Statements

1. Appropriate procedures shall be established for installation of web servers
2. Web servers shall be checked for any default / built-in user accounts before moving into production environment
3. All the unnecessary Services shall be disabled on the web servers
4. Access to web server root directory shall be restricted
5. Default files shall be removed from the web servers
6. Appropriate error messages shall be configured on the web servers
7. Directory surfing shall be disabled from the web browsers
8. Web servers shall be configured for an appropriate inactivity time-out
9. Concurrent connections on the web servers shall be defined as per the business requirements
10. Web servers shall be up-to-date with latest patches
11. Proper hardening of web servers shall be ensured
12. Caching of confidential information shall be forbidden on web servers
13. Confidential information shall not be hard coded on the web servers and source code viewing shall be disabled
14. Websites shall provide a warning message which will indicate that user is getting redirected
15. Web servers shall be protected against DOS attacks
16. Appropriate encryption shall be implemented on the web servers
17. Appropriate procedures shall be established for User and Authorisation Management Controls
18. Appropriate procedures shall be established for Password Management Controls

19. Appropriate procedures shall be established for Log Management Controls

20. Appropriate procedures shall be established for Backup Management Controls

6. Database Security Policy

Policy Objective

- To define appropriate controls to ensure that databases areadequately secured, logged and monitored.
- Database systems are kept with latest patches and upgrades
- Appropriate backup strategy is defined to ensure business continuity.

Policy Scope

This policy is applicable to all databases and is applicable to all users including the employees, contractors, consultants and temporary users.

Policy Statements

1. Ownership shall be established for each database
2. Appropriate procedures shall be established for installation and upgrade of databases
3. Access to database shall be controlled
4. Databases shall be monitored regularly
5. Transaction logs shall be monitored regularly
6. Critical databases shall be mirrored on separate disks
7. Appropriate procedures shall be established for backup / recovery of databases
8. Appropriate procedures shall be established for security of databases
9. Appropriate procedures shall be established for User and Authorisation Management Controls
10. Appropriate procedures shall be established for Password Management Controls
11. Appropriate procedures shall be established for Log Management Controls
12. Appropriate procedures shall be established for Backup Management Controls

7. Operating Systems Security Policy

Policy Objective

Establish adequate controls for the security of the operating systems and to ensure that they are duly protected against misuse and / or unauthorized access. This Policy is designed to ensure that

- Integrity of the Operating System is ensured.
- Access to the files, folders and other system utilities is controlled.
- Access to the operating system is controlled, logged, monitored and analysed.
- The Operating System is adequately protected against the threats of viruses and malwares

Policy Scope

This policy is applicable to all server and desktop Operating Systems and is applicable to all users including the employees, contractors, consultants and temporary users.

Policy Statements

1. Appropriate procedures shall be established for installation of operating systems

2. Minimum Baseline Security Standards or hardening standards for all Operating Systems and critical applications shall be defined, implemented and recorded

3. Access to operating systems shall be restricted

4. Appropriate procedures shall be established for file system design

5. Operating systems shall be updated with the prescribed operating system fixes and / or patches

6. Operation Systems shall be configured to timeout and clear the screen automatically

7. Each user shall be assigned a separate personal / home directory

8. Appropriate procedures for reporting information security incidents on the operating systems shall be established

9. Appropriate login process to Operating System, Application and Database shall be established

10. Correct setting of computer clocks shall be ensured

11. Appropriate procedures shall be established for Virus Protection

12. Appropriate procedures shall be established for User and Authorisation Management Controls

13. Appropriate procedures shall be established for Password Management Controls

14. Appropriate procedures shall be established for Log Management Controls

15. Appropriate procedures shall be established for Backup Management Controls

8. Network Security Policy

Policy Objective

- Only those services which are required for the business operations are enabled.
- Ensure integrity and availability of the network infrastructure.
- Ensure that the external connections (inward and outward) are controlled as per business requirements
- Private/trusted network is adequately protected against the threats from public/un-trusted network

Policy Scope

This policy is applicable to the LAN, WAN and all Network Devices like Switches, Routers, Firewalls etc. including Remote access to and from the network and is applicable to all users including the employees, contractors, consultants and temporary users.

Policy Statements

1. Ownership of network assets shall be established
2. Up-to-date network diagrams shall be maintained
3. Appropriate procedures shall be established to ensure that all the network equipment are tested before moving into production environment
4. IPs shall be based on network design
5. Appropriate procedures shall be established for segregation in network
6. Adequate redundancy shall be built into the network design
7. Default passwords of all network equipment shall be changed immediately after installation
8. Appropriate procedures shall be established for identification of network components
9. Appropriate procedures shall be established for network routing control
10. Appropriate procedures shall be established for packet filtering / blocking rules
11. Unused Interfaces, services and ports shall be disabled
12. Appropriate procedures shall be established for use of Firewalls, Intrusion Detection and Prevention System
13. Appropriate procedures shall be established for network monitoring
14. Appropriate procedures shall be established for network browsing
15. Appropriate procedures shall be established for access authentication

16. Appropriate procedures shall be established for safekeeping of network sniffers
17. Appropriate procedures shall be established for third party access to network
18. Appropriate procedures shall be established for remote access security
19. Appropriate procedures shall be established for remote diagnostic and configuration port protection
20. Appropriate procedures shall be established for network connection control
21. Appropriate procedures shall be established for User and Authorisation Management Controls
22. Appropriate procedures shall be established for Password Management Controls
23. Appropriate procedures shall be established for Log Management Controls
24. Appropriate procedures shall be established for Backup Management Controls

9. Internet Security Policy

Policy Objective

- To establish adequate security controls over access / usage of internet.
- Ensure that only authorised users are allowed access to the Internet.
- Ensure against malicious codes like viruses and worms
- To log and monitor the access to the internet.

Policy Scope

This policy is applicable to all the infrastructure assets which are used for the internet access like Proxy, Content Filtering Software, Network components etc. and is applicable to all users including the employees, contractors, consultants and temporary users.

Policy Statements

1. Access to internet shall be provided for business purpose only
2. Appropriate procedures shall be established for control over internet access
3. All the material downloaded from internet shall be screened by updated anti-virus
4. Appropriate procedures shall be established for internet log monitoring
5. Appropriate procedures shall be established for restricting abuse of internet access by users
6. Appropriate procedures shall be established for User and Authorisation Management Controls
7. Appropriate procedures shall be established for Log Management Controls

10. e-mail Security Policy

Policy Objective

- Implement adequate usage controls to ensure that the email facility is used only for the official purpose. e.g. content filtering, mail box size restrictions, mass mailing controls, attachment size controls etc.
- Protect the Information Assets from various threats related to the usage of E-mails like viruses, spam mails, leakage of information through e-mails etc.
- E-Mail usage should be logged and monitored.
- To encourage an efficient communication system and to add value to the services offered by SNDTWU.
- Implement adequate security controls to ensure that the vulnerabilities associated with email facility are minimized e.g. antivirus etc.

Policy Scope

This policy is applicable to the infrastructure supporting the E-mail services like E-Mail Server, Mail Box server, E-Mail application, etc. and is applicable to all users including the employees, contractors, consultants and temporary users.

Policy Statements

1. Appropriate procedures shall be established for controlling e-mail access
2. Users shall access only the approved client email software
3. Users shall not abuse e-mail access
4. Appropriate procedures shall be established for restricting access to other user's e-mail account
5. Users shall not open e-mails / attachments received from unknown source
6. All incoming and outgoing mails shall be scanned for viruses and content filtering
7. SNDTWU can inspect the email and attachment contents of any user at any time without notice
8. Auto forwarding of e-mails shall be restricted
9. Sending of critical information through e-mails shall be controlled
10. Attachment size of e-mails shall be restricted
11. Every e-mail shall contain a standard and approved disclaimer
12. Every user shall adopt standard e-mail signature approved by SNDTWU
13. Appropriate procedures shall be established for ensuring proper backups of e-mail files
14. Access to Emails from outside of SNDTWU's Network shall be controlled
15. Controls over distribution email Ids shall be established

16. Appropriate procedures shall be established for securing and maintaining e-mail logs

17. Appropriate procedures shall be established for User and Authorisation Management Controls

18. Appropriate procedures shall be established for Password Management Controls

19. Appropriate procedures shall be established for Log Management Controls

20. Appropriate procedures shall be established for Backup Management Controls

11. Desktop and Laptop Security Policy

Policy Objective

- To ensure adequate control over usage of SNDTWU’s desktops and laptops.
- To protect information systems and assets through appropriate controls over usage of external media and software applications.
- To ensure that the end-user who has been allotted a desktop / laptop is made aware of his / her responsibility towards the usage of those asset.
- To reduce the risk of theft of assets / data by maintaining secure environment.

Policy Scope

This policy is applicable to all geographical units of SNDTWU and to all users.

Policy Statements

1. Desktops / Laptops issued to staff or consultants remain the property of SNDTWU
2. Appropriate procedures shall be established for ensuring security of desktops / laptops
3. Installation of software on desktops / laptops shall be controlled
4. Users shall return the desktop / laptop while leaving employment of SNDTWU

12. Clear Desk Clear Screen Policy

Policy Objective

The objective of the policy is to ensure that the Desktops, Laptops, paper and computer media containing confidential information and all associated equipment are stored suitably in a secured manner when not in use to reduce the risk of unauthorized access.

Policy Scope

The policy applies to:

- All the information of SNDTWU regardless of whether it is stored electronically or in paper format.
- All users
- All associated equipment of SNDTWU like computers, or terminals, facsimile machines, photocopiers, printers etc.

Policy Statements

1. Appropriate procedures shall be established for clear desk
2. Appropriate procedures shall be established for protection of personal items of users
3. Appropriate procedures shall be established for securing prints
4. Appropriate procedures shall be established for preventing unauthorised access to information discussed during meetings
5. Appropriate procedures shall be established for clear screen
6. Appropriate procedures shall be established for laptop security
7. Appropriate procedures shall be established for protection of paper and removable media
8. Need-to-know policy shall be implemented

13. Virus Protection Policy

Policy Objective

The Virus Protection Policy is designed to ensure that

- Anti-Virus Software is installed on all Servers, Personal Computers, Laptops, E-Mail Servers, Proxies and Internet gateways.
- Only licensed and authorized AV software is being used.
- Any external device should be scanned before allowing on the Network.
- An incidence response procedure is defined in case of a virus attack on the set up.

Policy Scope

This policy is applicable to all geographical units of SNDTWU and to all users.

Policy Statements

1. Procedures shall be established for selection of appropriate Anti-Virus Software
2. Anti-Virus Software shall be installed on all servers and workstations of SNDTWU
3. Appropriate procedures shall be established for Anti-Virus controls over the Development and Test environments
4. Appropriate procedures shall be established for ensuring appropriate Anti-Virus Software settings
5. Anti-Virus Software shall be installed on all mobile computing devices of SNDTWU
6. Appropriate procedures shall be established for third party laptops connecting to SNDTWU's network
7. Appropriate procedures shall be established for reporting of virus infections
8. Appropriate procedures shall be established for handling virus incidents
9. Procedures shall be established for ensuring appropriate Anti-Virus awareness among the users
10. Appropriate procedures shall be established for controls over mobile code

14. User and Authorisation Management Policy

Policy Objective

The objective of this Policy is to ensure that

- User Management is standardized and governance controls are implemented over the Registration, Modification and De-registration of users.
- Access/authorisation should be granted to the users as per business requirements and only against approval from the designated authority.
- Users are informed about their legitimate accesses and also educated about the consequences of access violations.
- Reviews are done of the user management process.

Policy Scope

This policy is applicable to all geographical units of SNDTWU and to all the users

Policy Statements

1. Appropriate procedures shall be established for control over default users
2. Appropriate procedures shall be established for user creation, modification and deletion
3. Appropriate procedures shall be established for identification of dormant and inactive user ids
4. Appropriate procedures shall be established for assigning roles and groups to users
5. Each user Id shall be uniquely identified on a system
6. Appropriate procedures shall be established for control over generic user ids
7. User ID shall be locked after three failed logging attempts
8. Appropriate procedures shall be established for control over temporary user ids
9. User inactivity time out shall be configured
10. Adequate segregation of duties shall be enforced
11. Regular review of Users and their Privileges shall be carried out

15. Password Management Policy

Policy Objective

The objective of this policy is to define and implement adequate authentication controls in the form of good password controls and disciplines.

Policy Scope

This policy is applicable to all geographical units of SNDTWU and to all the users.

Policy Statements

1. SNDTWU shall implement strong encryption algorithm for passwords
2. All the default passwords shall be changed before moving any system in production environment
3. Minimum password length shall be enforced
4. The System shall inform the user that his / her password would be due for change
5. Users shall be forced to change their passwords after passwords are reset
6. Users shall be forced to change their passwords after first login
7. The System shall enforce change of password composition
8. The System shall be configured to disallow a user to change his / her password for a pre-defined minimum period
9. Users shall be forced to change their passwords at regular intervals
10. The System shall enforce alpha-numeric password composition
11. The System shall enforce password complexity
12. The users shall not share their passwords
13. Procedural password controls shall be implemented
14. Users shall have the option of changing their passwords
15. The System shall not allow the users to select any of their pre-defined number of passwords
16. Critical passwords shall be available even when the concerned administrator is on leave or not available

16. Log / Audit Trail Control Policy

Policy Objective

This Policy is developed to ensure that

- Audit Trails / Logs capture adequate details like the user ID, Activity of the user, the location identifier and the Date and Time Stamp to ensure accountability.
- System Logs should help in analysing the performance and other issues.
- Audit Trails / Logs are secured against unauthorized modifications.
- The time stamping of logs should be done with the network time server (Clock Synchronization)
- Audit Trails / Logs should be retained for the defined period.
- A process of analysing and monitoring the logs to identify security incidents and operational problems is defined and implemented.

Policy Scope

This policy applies to all logs generated by the application systems, Database, operating systems, network components, including the physical access logs maintained in manual registers and surveillance systems.

Policy Statements

1. Log management strategy shall be defined
2. Appropriate procedures shall be established for capturing necessary details
3. Appropriate procedures shall be established for appropriate log analysis
4. Adequate disk space for logs shall be maintained all the time on respective systems
5. Common network time stamping shall be used
6. Strict access controls over log files shall be established
7. All critical Log files shall be opened in Append mode
8. Critical Logs shall be preserved for pre-defined approved retention period
9. In case of investigations, the critical log files shall be preserved for the required period as per directions of relevant authorities
10. Log host shall be defined
11. List of critical logs to be monitored shall be prepared

17. Backup Management Policy

Policy Objective

- To ensure that a business requirement driven backup Strategy is defined and implemented.
- To ensure that appropriate backups of the relevant systems are available, in case of failure of the production environment.
- To ensure that the backups are tested for readability / restoration at regular intervals.
- To ensure that adequate sets of backups are taken for critical information assets and at least one set is stored at the identified off-site locations.

Policy Scope

- Backup process for servers, applications, databases, network components, and critical personal computers.
- Labelling, storage, handling and movement of backup media.
- Testing and restoration of the backup media.
- Recycling and destruction of the backup media.

Policy Statements

1. Responsibility of defining backups shall be defined
2. Appropriate procedures shall be established for making changes to backup requirements
3. One nodal person shall be appointed for coordinating all backup and restoration related activities
4. Appropriate procedures shall be established for obtaining vendor support when required
5. Each backup request shall be approved by relevant authority
6. Backup responsibility shall be defined
7. Appropriate procedures shall be established for temporary backups
8. Appropriate procedures shall be established for review of backups
9. Inventory of backup media shall be maintained
10. Appropriate procedures shall be established for choice of backup media and backup application
11. Appropriate procedures shall be established for rotation / recycling of backup media
12. Backup media shall be stored as per specification received from the respective vendor

13. Appropriate procedures shall be established for control over movement of backup media

14. Appropriate procedures shall be established for testing of backup media

15. Appropriate procedures shall be established for testing complete restorability / recoverability

16. Appropriate procedures shall be established for retiring of backup media

17. Appropriate procedures shall be established for physical destruction of backup media

18. Physical and Environmental Security Policy

Policy Objective

Objective of the policy is to define the requirements for protecting SNDTWU's information and technology resources from physical and environmental threats like the risk of loss, theft, damage, or unauthorized access.

Policy Scope

This policy is applicable to all geographical units and to all the users of SNDTWU

Policy Statements

1. Access restrictions to secure areas should be established
2. Critical equipment / areas should be secured
3. Identification badges should be mandatory for gaining access to premises
4. Security guards must be stationed at the main entrance of the "Secure Areas"
5. Appropriate procedures for visitors access should be established
6. Appropriate procedures for temporary / lost / stolen identity badges should be established
7. Appropriate physical access restrictions should be established
8. Clearance procedures for terminated / resigned employees should be established
9. Security of cables / electrical fittings should be ensured
10. Systems for fire detection / suppression should be established
11. Systems for controlling water damage should be established
12. Cleanliness of premises should be ensured
13. Appropriate procedures for handling power outages should be established
14. Appropriate procedures for handling equipment with due care should be established
15. Physical security of workstations / laptops should be ensured
16. Equipment should be maintained in such a way to ensure its continued availability and integrity
17. Secure Disposal or re-use of equipment should be ensured
18. Public access, delivery, and loading areas should be secured