Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

Information Security Management System

Password SOP

Password SOP

Ministry of Information Technology & Telecommunication
DIGITAL PAKISTAN

Document Control

Prepared / Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval

Change History

SN	Version	Changes Description
1	**1.0**	**Final Version**

Document Approval

Sr. No	Approver (Name/Title)	Signatures
1		
		Date:
2		
		Date:
3		
		Date:
4		
		Date:

Ministry of Information Technology & Telecommunication
DIGITAL PAKISTAN

Table of Contents

1 Abbreviations

BCP: Business Continuity Plan

SLA: Service Level Agreements

HoD: Head of Department

Anti-X: Anti- Virus, Anti-Malware, Anti- Spam, Firewalls etc.

IT Security: Information Technology Security Team

DLP: Data Leakage/Loss Prevention

2 Abstract

This document contains the policies and procedures that concern password security usage within the organizations of Government of Pakistan. While some of the policy items can be enforced by configurations, it is important for all users to recognize and use these procedures to ensure the security of the information resources.

The document also describes audit requirements in terms of approvals and log records to enable cross-checks on account and password creation, modification and deletion.

3 Introduction

3.1 Background

Access to computing resources and data are controlled by user account identifiers (User-ID's) and Passwords. This is the primary identification process. The identification processes are one of the most important components in the information security policy, which is required to ensure protection of information and technology systems.

3.2 Objectives

In order to ensure correct usage of accounts, linked to individual biometric parameters (if applicable) and to passwords, all users are required to understand the security ID and password policy.

3.3 Readership

All staff must be familiar with and follow the procedures outlined here to help ensure protection of information resources and systems. Nominated staff will be required to implement as much control over password structure via configuration as possible.

4 Policy

The following rules govern an individual's identification and the password policy:

1. Systems shall be set to lock out further logon attempts for at least 15 minutes or after five consecutive failed username or password attempts have occurred.
2. The logon sequence provided by each operating system will require the entry of the User ID and password, each at appropriate prompts.
3. Security audit must be enabled on each operating system (if applicable) to record the following security alerts:

   a. Logon and Logoff events - success and failure
   b. Resetting of passwords
   c. Changing any of the user attributes (i.e. Win user profile)

4. All user level passwords should be created with the following characteristics:

   a. Accept and support as a minimum password consisting of 8 non-blank printable characters drawn from 3 out of the following 4-character sets:
      i. English upper case.
      ii. English lower case.
      iii. Numeric characters (0 to 9).
      iv. Special (printable) characters.

   b. Users are empowered to change their passwords, and Maximum Password age could be up to 60 days.

   c. Users are allowed and encouraged to select passwords longer than 8 characters if they wish.

   d. If the password needs to be sent across Network that should be encrypted/hashed.

   e. If shared passwords are authorized in exceptional circumstances, they must be changed promptly whenever one of the users ceases to be authorized for its use.

   f. The auto complete option of web browser forms should be disabled.

   g. The Password should not be saved in Web Browse forms, or any kind of tools or software to access the critical Information resources.

   h. Passwords or other information that might assist unauthorized access to computer terminals or printers. Passwords must not be recorded in audit trails or logs.

5. All user passwords for core/critical servers and devices should be created with the following characteristics:

   a. Accept and support as a minimum password consisting of 10 non-blank printable characters drawn from 3 out of the following 4-character sets:

      i. English upper case.
      ii. English lower case.

iii. Numeric characters (0 through 9).
iv. Special (printable) characters.
v. Avoid dictionary and easily guessable words (e.g myname12345678)

b. Administrator are empowered to change the passwords and Maximum password age is 14 days.

c. The administrative credentials for Servers and critical Services should never be saved in any kind of administrative tools and software.

d. The sharing of Administrative Passwords of the critical Servers and Network Devices should be strictly prohibited.

e. The LOG-ON banner should be used, to intimate the logging in user, that Only Authorized personnel can log in.

6. If password needs to be shared over the network, it must be ensured that file is protected with password or encrypted.
7. Passwords used within the department's systems must not be used on other systems outside the department.
8. Passwords (and thus accounts) must not be shared with others.
9. Passwords must not be stored in readable form in batch files or other locations without special security precautions that take this requirement into account.
10. All service vendor default passwords must be automatically disabled upon completion of on-site system service.
11. If a suspected disclosure of passwords has occurred, all involved account passwords shall be immediately changed, the users informed and the action entered in the Account Logbook.
12. When a user calls for a password reset, the relevant person will call the user back to confirm their request before proceeding.
13. New passwords will be issued in a state that requires it to be changed when the user logs on to the system for the first time.
14. All above policies are applied to the following operating environments:
    i. Windows Passwords,
    ii. Screen Saver Passwords and
    iii. Password secured applications.
15. Any application that implements specific username and password routines must also comply with the above policies. It is the sole responsibility of the Applications Administrator and users of the applications to adhere to the above policies.
16. Any staff member, who uses a privileged account, must have another normal, non-privileged, account for normal daily operations that does not require special privileges.

17. Any staff member, who requires a privileged account, should be granted only the appropriate privileges to carry out their assigned duties.
18. System and Administrator level accounts must be held and used only by the Windows Administrator and must not be shared with others.

5 Password Creation and Use

1. Every user account must be created using the Account Maintenance Form (AMF) or request through security manager (software), which must be signed by the user and user's Manager or IT Coordinator.
2. On the receipt of the new password, the user must sign the AMF, a copy of which is maintained by Network and Infrastructure Division.
3. All user access to department's information systems and network systems must be carried out via allocated user account.
4. All account passwords must be memorized, never written down.

6 Password Modification

Occasionally Technical support may be called upon to reset a user's password. (e.g. user changes his password just before going on vacation and then cannot remember it when he returns from vacation). The following procedure must be followed whenever DC technical support Technical Operations have to reset a user's password:

1. The operator must verify that the user requesting the password reset is the actual owner of the account.
2. The operator sets a new password for the account. The password must be pre-expired so that the user is forced to change the password when logon process is attempted for the first time after the password has been reset.
3. If the password is not reset in the presence of the account owner, it will be passed to him verbally or by telephone within the department's building only.
4. Passwords are not to be shared with others. This practice is not allowed. If a temporary access is required to an account by other than the owner of the account (e.g. secretary left on vacation), an email must be sent by the relevant IT Coordinator or Department Manager.
5. When using a temporary password, the system should disable the option for the user to update the biometric (fingerprint) details for that account (if applicable).

7 Audit Requirements

All requests must be logged in security management log and kept available for audit, and at any time, by relevant authorized authorities.

Document Title	Access Request Form

This form should be completed when requesting authorisation for access to network/VPN account or for making changes to any existing access, removing access if a user leaves the department or for a user name change.

The form should be completed and forwarded to Help desk, in person, by post or by scanning and sending to IT Support email address of the department.

Ministry of Information Technology & Telecommunication
DIGITAL PAKISTAN

User Details

First Name	
Last Name	
CNIC	
Employee/Customer ID	
Designation	
Organization	
Department	

Contact Details

(Please enter an email address or phone number so that we can contact you if we need any further information or when the access has been granted).

Telephone Number	
Email Address	

Nature of Access Request (tick):

New or Additional Access		**Disable Access (Access no longer required)**	
Modify Existing Access		**Other (please specify)**	
Request Date:			
Type of Access (VPN/Server Room or Network):			

Access Required (please list below access affected by this request)
(Tick 'Add', 'Remove' or 'Modify' as appropriate and indicate if Read Only (RO) or Read/Write (RW))

User, Network Resource, Server Room, Folder or Path	RO / RW	Add	Remove	Modify

Access Authorisation (ISO/Nominated Authorised Person)

Access Authorised By (name):	
Access Authorised By (Signature):	
Approval Date:	