ADIB – Standard

(UAE, Qatar, Iraq, Sudan, and UK)

Password Security Standard

STD-ITD-552

Date: 30th January 2024
Version: 6.2

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
6.2	30th January, 2024	No change required	Annual review
6.1	30th April, 2023	Document has been reviewed and ensured is up to date	Document review cycle
6.0	30th April, 2022	Updated "Maximum password age" & "Session Idle Timeout"	Process alignment with current practices
5.0	30th January, 2022	Cloud password management Added Password guidelines for cloud administrators & users	Cloud Adoption
4.3	October, 2021	Document has been reviewed and ensured is up to date	Document review cycle
4.2	Publishing Date	Document is up to date. No change required.	Process review cycle
4.1	Publishing Date	Document has been reviewed and ensured is up to date	Document review cycle
4.0	Publishing Date	Moved document to new format. Updated controls: Added clause for third party and password complexity Modified controls to synergies password length etc.	Process alignment with current practices
3.0	Publishing Date	GARR findings for database security controls	GARR points addressed
2.2	Publishing Date	ISO27001:2005 changed to ISO27001:2013	IMS Update
2.1	Publishing Date	Streamlining of complete Standard	Process Optimization

Prepared by	Approved by	Reviewed by
Governance Team	Head of IT Compliance and Security Architecture	IT Governance Manager

Contents

Version Control & Change Management 2
1 Overview 4
2 Applicability 4
3 Standard Owner 4
4 Standard Statements 4
4.1 Password Selection 4
4.2 Password Storage 4
4.3 Password Management for Master IDs 4
4.4 Password Transmission 5
4.5 Password Change 5
4.6 ADIB Domain Password 5
4.7 System Account Passwords 6
4.8 Application Passwords 6
4.9 Database Passwords 7
4.10 Password Complexity 7
4.11 Network Device Passwords 8
4.12 Third-Party Password Management 8
4.13 ATM OS / BIOS Password Management 8
4.14 Cloud Password Management 8
4.15 Password guidelines for cloud administrators 8
4.16 Password guidance for cloud users 9
5 Exceptions 9
6 Appendixes 9
Annex I: Definitions 9

1 Overview

The objective of this standard is to set a benchmark for selection, use and protection of passwords across ADIB ITD.

2 Applicability

This standard is applicable to ADIB ITD UAE, Qatar, Iraq, Sudan, and UK.

3 Standard Owner

Head of Compliance and Security Architecture

4 Standard Statements

4.1 Password Selection

1. All passwords, irrespective of the platform, should be at least 8 characters long.
2. Passwords used by privileged accounts should be at least 10 characters in length, wherever technically possible.
3. Wherever possible passwords should be case sensitive.

4.2 Password Storage

1. Information processing systems should store passwords in one-way hashed form
2. Information processing systems should maintain a history of last 10 passwords for each user account.
3. Passwords should always be encrypted using one of the following methods:
   a. Non-reversible encryption – in this mode the password can never be decrypted by any entity. The server can only compare the encrypted values OR
   b. reversible encryption – the key for decryption should also be secured in a way that it is not visible on client machines for e.g., utilize operating system provided mechanism for encryption and key storage
4. Encoding, obfuscation, custom techniques to hide the password shall not be used for securing passwords and keys.

4.3 Password Management for Master IDs

1. Password for Master IDs should be held individually, in tamper- evident envelopes & the envelopes should be kept in a fireproof safe under the dual custody of Head of IT GRC and Head of T&CS, which would prevent the access or knowledge of the password to any single individual.
2. Master ID to be used only for emergency purposes (applicable to all systems where this requirement is supported). System Administrators should use their own ID for all system administration activities.
3. Once the Master ID password is used, it should be reset by the user and the new password to be recorded and kept in the fireproof safe.
4. All Master ID passwords should be reset and replaced in the safe, annually, between February & March of every year.

4.4 Password Transmission

1. Passwords should not be shared with anyone
2. Passwords should not be transmitted through any medium
3. Administrators should consider communicating temporary passwords to users via encrypted email messages, through mails sealed with tamper-proof envelope. Any written form of password should be physically destroyed

4.5 Password Change

1. All information processing systems should enforce users to change their passwords periodically as per the platform-specific standards in the following section.
2. All information processing systems should restrict users from reusing previously used passwords, as per the platform-specific standards in the following section.

4.6 ADIB Domain Password

1. All production servers, desktops and laptops should be part of the Windows domain operated by ADIB ITD.
2. Wherever technically possible; password complexity should be configured to enforce usage of alphanumeric characters, as the minimum requirement for creation of passwords.
3. Domain level password policies should be enforced as below.
   - Enforce password history – 10 passwords
   - Maximum password age
     - o ADIB Group Heads and ADIB Leaders Group – 60 Days
   - o All Other Users – 45 Days Minimum password age – 1 day
   - Minimum password length – 8 characters
   - Passwords must meet complexity requirements – Enabled (Wherever technically possible)
   - Failed Logon Attempts – 5
   - Account Lockout duration – 15 minutes
4. The following settings should be enforced as a part of account lockout policy
   - Account lockout duration – 30 minutes
   - Account lockout threshold – 5 invalid login attempts
   - Reset account lockout threshold after – 30 minutes
5. Test accounts should be subjected to the Domain password policy with the exception of the following parameter:
   - Maximum password age – 180 days
6. Windows guest account should be disabled on all Windows desktops, laptops and servers.
7. Privileged accounts should not make use of default names such as Administrator.
8. Domain level policies should be configured on all user desktops, laptops and servers to enforce use of screen saver password and be activated after defined idle time, unless authorized otherwise. Session Idle Timeout is defined as below

   o ADIB Group Heads – 10 Minutes.

- All Other Users – 5 Minutes.

4.7 System Account Passwords

1. Service accounts should be subjected to the following password policy settings:
   - Enforce password history – Not Configured/ Unlimited
   - Maximum password age – Not Configured/ Unlimited
   - Minimum password age – Not Configured/ Unlimited
   - Minimum password length – 10 characters
   - Passwords must meet complexity requirements – Enabled
2. Service account shall be used by applications only and not be used by administrators or other users. Service account activity shall be monitored to identify & alert any logon activity seen from service accounts which is not initiated by application systems. Local Administrator accounts should be subjected to the following password policy settings:
   - Enforce password history – Not Configured/ Unlimited
   - Maximum password age – 1 year (To be changed in line with the 'Master ID Reset' activity outlined in Section#3 above)
   - Minimum password age – Not Configured/ Unlimited
   - Minimum password length – 8 characters
   - Passwords must meet complexity requirements – Enabled

4.8 Application Passwords

1. Administrators should ensure that default passwords of applications are changed after installation.
2. Wherever local authentication on the application is inevitable, the application should be configured to comply with the following:
   - All customer facing applications should support a "Forgot password" module to reset user passwords in a secure fashion:
     - For customer facing applications where user forgets his/her password, the user should access the 'forgot password' option and provide information / details which substantiate his/her authenticity. On satisfactory verification, the application should mail the new password to the user.
     - In case the email is required to be sent, then email should not contain the new password of the user but should contain a link to enter the new password. The link should be active for only a day and should be disabled after that.
3. All applications should encrypt passwords
4. All applications should disable the "Remember password" feature of web browsers, using appropriate scripts.
5. All internet facing applications should enforce strong password policies, as mentioned below, unless business requires different setting based on risk acceptance:
   - Enforce password history – 10 passwords
   - Maximum password age – 365 days

- Minimum password age – 1 day
- Minimum password length – 8 characters
- Passwords must meet complexity requirements – Enabled

6. All internally accessed intranet-based applications which are not integrated with Active Directory for Single Sign-on should enforce password policies

7. All applications, wherever technically possible, should enforce strong account lockout policies, as mentioned below:

   - Account lockout duration – 30 minutes
   - Account lockout threshold – 3 invalid login attempts
   - Reset account lockout threshold after – 30 minutes

8. All packaged or customized software bought from external vendors, wherever possible, should provide provisions to configure strong password policies as mentioned above.

4.9 Database Passwords

1. Database Administrators should ensure that default usernames and passwords are changed or removed from the database after installation.

2. All databases should store user credentials in encrypted form

3. All databases should use the Windows authentication mechanism, wherever technically possible, to ensure enhanced security, instead of mixed or standard authentication.

4. Wherever Windows authentication is not technically enforceable, the following password and account lock out policies should be implemented:

   - Failed Login Attempts- 5
   - Lifetime of a password - 35 days
   - The time limit before a previous password can be re-entered- 1
   - The maximum number of times a password can be used- 1
   - The time duration for the account to remain locked, after the failed login attempts limit is crossed - 30 minutes
   - The grace period after the lifetime of a password is exceeded- 0

5. Any user-initiated service account activity to ADIB critical databases shall be monitored.

4.10 Password Complexity

1. The password complexity should be as following Minimum 8 characters

2. Complexity should be at least three of below mentioned four conditions
   a. one Capital Letter
   b. one special character
   c. one number and
   d. one small letter

3. Should not be easily guessable i.e., your name, date of birth, department name, cell number

4.11 Network Device Passwords

1. Network Administrators should ensure that default users name and passwords are removed from all network devices after installation.
2. All network devices should store passwords only in encrypted form in their configuration files.

4.12 Third-Party Password Management

1. Service Accounts
    a. The password expiry shall be one year for service accounts.
    b. Any exception shall be documented
2. Administrative Accounts
    a. The password expiry shall be 35 days
3. Associated AD accounts and service accounts shall also expire on expiry of user credentials of ADIB Third-Party vendors

4.13 ATM OS / BIOS Password Management

1. The expiry of ATM OS password should be set to 365 days
2. The expiry of BIOS password should be 365 days

4.14 Cloud Password Management

1. Inventory of all administrative accounts shall be maintained
2. Enforce to change default passwords
3. Ensure the use of dedicated administrative accounts
4. Enforce to use Unique Passwords
5. Implement multi-factor authentication for all administrative access
6. Configure Limit Access to Script Tools accessing the passwords.
7. Configure Log and alert on changes to administrative group membership
8. Configure Log and alert on unsuccessful administrative account login
9. Implement approval process and workflow for cloud account access (like PIM in Azure)
10. Detect & Alert on IAM Logins without MFA, and IAM Logins that don’t come from known IP Addresses
11. Leverage of SSO and Federation for console and cloud native resources API Access in cloud systems
12. Ensure API password management for App Services with respective service principles account using key vault.

4.15 Password guidelines for cloud administrators

1. 8-character minimum length password requirement shall be maintained
2. Ensure the usage of password with correct standards with proper character composition requirements.
3. Enable common passwords usage restrictions to keep the most vulnerable passwords out of cloud system
4. Educate the users to not re-use ADIB cloud passwords for non-work-related purposes
5. Enforce multi-factor authentication for cloud privileged accounts.
6. Enable risk-based multi-factor authentication challenges

7. Wherever Cloud AD authentication is technically enforceable, the following password and account lock out policies shall be followed as per cloud provider standards:

   a. Failed Login Attempts - 10
   b. Lifetime of a password - 90 days
   c. The maximum number of times a password can be used - 1
   d. The time duration for the account to remain locked, after the failed login attempts limit is crossed - 60 minutes
   e. The grace period after the lifetime of a password is exceeded – 0

4.16 Password guidance for cloud users

1. 8-character minimum length password requirement shall be maintained
2. Ensure the usage of password with correct standards with proper character composition requirements.
3. Wherever Cloud AD authentication is technically enforceable, the following password and account lock out policies shall be followed as per cloud provider standards:

   a. Failed Login Attempts- 10
   b. Lifetime of a password - 90 days
   c. The maximum number of times a password can be used - 1
   d. The time duration for the account to remain locked, after the failed login attempts limit is crossed - 60 minutes
   e. The grace period after the lifetime of a password is exceeded – 0

5 Exceptions

Any deviation to the standard shall be documented along-with associated risks and shall be approved

6 Appendixes

Annex I: Definitions

1. **Privileged Account**s refer to accounts that have elevated access privileges such as local/domain administrator accounts etc.
2. **Master IDs** are privileged accounts with the highest level of access privileges and can be used to perform any and all operations within the respective system