	Password Policy			
	Document Code: INFS-POL-23	Document Classification: Confidential	Version No: 1.0	Date: Jan-2023

Purpose:

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change across all Information and Communication Technologies and related systems throughout SCAD.

Scope:

This policy applies to all employees (permanent & contract employees) and non-employees (consultants, contractors, vendors, suppliers, and customers) and partner agencies who have access to SCAD's systems, equipment, and devices.

Policy:

All SCAD information resources will have appropriate password controls in place to safeguard the assets from unauthorized or illegal access.

Password Creation:

1. All passwords, irrespective of the platform, should be at least 14 characters long.
2. Users should make use of passphrases instead of normal passwords.
3. Passphrases used by privileged accounts should be at least 14 characters in length.
4. Passwords are case sensitive, and the password strength can be increased if mixed-case passwords are used.
5. Another strategy for creating strong passwords is to replace letters with numbers or symbols. For example SecDsk5 becomes \$e6D\$k5 where the letter "c" has been replaced with the digit "6" and the letter "s" has been replaced with the symbol "\$".
6. The above guidelines for password creation should be followed for operating systems, applications, databases and network devices.


Password Storage

1. Information processing systems should store passwords in one way hashed form.
2. A particular password should be maintained in active state only for a pre-defined period.
3. Information processing systems should maintain a history of a pre-defined number of previously used passwords for each user account.

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

Prepared By Information Security Team	Reviewed By Director Information Security Office	Approved By Director Information Security Office	Released By Corporate Strategy & Excellence	Page 1 of 5
---	--	--	---	-------------

	Password Policy			
	Document Code: INFS-POL-23	Document Classification: Confidential	Version No: 1.0	Date: Jan-2023

Local Admin password on Desktop/Laptops

1. There will be only one local admin account on any Desktop laptop
2. IT technicians, with their own domain account, will have local administrator privileges on user machines to perform troubleshooting & installation activities.


Windows Domain Passwords


1. All Windows servers, desktops and laptops should be part of the Windows domain operated by SCAD. Domain level password policies should be enforced on all Windows servers, desktops and laptops to ensure use of strong and complex passwords.
2. Domain level policies should be enforced on all windows servers, desktops and laptops to prevent wrong use of passwords to gain unauthorized access to user accounts.
3. The following settings should be enforced as a part of account lockout policy
 - a) Passwords must meet complexity requirements – Enabled
 - b) Account lockout duration – 30 minutes
 - c) Account lockout threshold – 5 invalid login attempts
 - d) Reset account lockout threshold after – 30 minutes
4. Privileged accounts should be enforced with following password policy:
 - a) Enforce password history – 10 passwords
 - b) Maximum password age – 60 days
 - c) Minimum password age – 1 days
 - d) Minimum password length – 14 characters.
5. Privileged accounts should be enforced with following account lock out policy:
 - a) Passwords must meet complexity requirements – Enabled
 - b) Account lockout duration – 30 minutes
 - c) Account lockout threshold – 3 invalid login attempts
 - d) Reset account lockout threshold after – 30 minutes
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 5 minutes of idle time.

Application Passwords

1. Application administrators should ensure that default passwords of applications such as IIS, WebLogic, Apache, E-Services, Intranet Portal, HR, Finance etc. are removed after installation.
2. All external applications should support a “Forgot password” module to reset user passwords in a secure fashion.

Prepared By Information Security Team	Reviewed By Director Information Security Office	Approved By Director Information Security Office	Released By Corporate Strategy & Excellence	Page 2 of 5
---	--	--	---	-------------


 مركز الإحصاء STATISTICS CENTRE	Password Policy			
	Document Code: INFS-POL-23	Document Classification: Confidential	Version No: 1.0	Date: Jan-2023

3. All applications should encrypt passwords using salted hash techniques before transmitting them over the network. 
4. All applications, wherever possible, should disable the “Remember password” feature of web browsers, using appropriate scripts.
5. All publicly accessible web based applications, wherever technically possible, should implement the CAPTCHA module for user authentication apart from regular username and password.
6. All critical applications should implement the HTTPS module for user authentication and other critical data transmission.
7. All publicly accessible Internet based applications, wherever technically possible, should enforce strong password policies:
 - a) Enforce password history – 10 passwords
 - b) Minimum password age – 1 days
 - c) Minimum password length – 14 characters
8. All internally accessed intranet-based applications, wherever technically possible and if not integrated with Active Directory for Single Sign-on, should enforce strong password policies as follows:
 - a) Enforce password history – 10 passwords
 - b) Maximum password age – 120 days
 - c) Minimum password age – 1 days
 - d) Minimum password length – 14 characters
9. All applications, wherever technically possible, should enforce strong account lockout policies:
 - a) Account lockout duration – 30 minutes
 - b) Account lockout threshold – 5 invalid login attempts
 - c) Reset account lockout threshold after – 30 minutes
10. All packaged or customized software bought from external vendors, wherever possible, should provide provisions to configure strong password policies as mentioned above.

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 such as passwords, authentication codes or personal identification numbers (PIN) in encrypted one way hashed form.
3. All databases should encrypt passwords using salted hash techniques before transmitting them over the network.
4. All Oracle databases should enforce strong password and account lock out policies:
 - a) FAILED_LOGIN_ATTEMPTS 3
 - b) PASSWORD_LIFE_TIME 60 days
 - c) PASSWORD_REUSE_TIME 90 days

Prepared By Information Security Team	Reviewed By Director Information Security Office	Approved By Director Information Security Office	Released By Corporate Strategy & Excellence	Page 3 of 5
--	---	---	--	-------------

	Password Policy			
	Document Code: INFS-POL-23	Document Classification: Confidential	Version No: 1.0	Date: Jan-2023

- d) PASSWORD_REUSE_MAX 5
- e) LOCK_TIME - Account lock for 30 mins after 3 unsuccessful logon
- f) PASSWORD_GRACE_TIME - 7 days to change the password after 60days
- g) PASSWORD_VERIFY_FUNCTION VERIFY_FUNCTION;

5. All SQL server databases should use Windows authentication mechanism to ensure enhanced security, instead of mixed or standard authentication.


6. In case of difficulties of implementing password policy, deviations have to be reported to CISO and approval should be obtained.

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.

3. All network devices should be configured for remote administration only using secure SSH protocol. This will ensure that user credentials such as usernames and passwords are sent in encrypted form during remote administration session.

4. All network devices should be configured for secure user authentication using TACACS or RADIUS server to ensure traceability in administrative activities. 

5. All network devices using services based upon SNMP protocol should ensure that default community strings are replaced with stronger and complex strings.

6. All network devices, wherever technically possible, should enforce strong password policies:

- a) Maximum password age – 90 days 
- b) Minimum password age – 0 days
- c) Minimum password length – 14 characters

7. All network devices, wherever technically possible, should enforce strong account lockout policies:

- a) Account lockout threshold – 3 invalid login attempts
- b) Account lockout duration – 30 minutes

UNIX Server Passwords

1. Days before a forced password change that a warning will be given to the user informing them of the impending password change = 7.

2. Maximum number of Days a password is valid – 180 days.


3. Minimum length of a password – 10

4. Minimum number of non-alphabetic characters in a password) – 1.

5. Minimum number of alphabetic characters in a password) – 1

6. Number of previous passwords which cannot be reused -10.

Prepared By Information Security Team	Reviewed By Director Information Security Office	Approved By Director Information Security Office	Released By Corporate Strategy & Excellence	Page 4 of 5
---	--	--	---	-------------

	Password Policy			
	Document Code: INFS-POL-23	Document Classification: Confidential	Version No: 1.0	Date: Jan-2023

Password Policy

1. Require a change of initial or “first-time” passwords

- Forcing a user to change their initial password helps ensure that only that user knows his or her password.
- Depending on what process is being used to create and distribute the password to the user, this practice can also help mitigate the risk of the initial password being guessed or intercepted during transmission to the user.
- This guidance also applies to situations where a password must be manually reset.
- The Human Resources request the infrastructure team to create user ID for new employees

2. Always verify a user’s identity before providing the initial password

- A user’s identity should always be validated prior to providing the initial password.
- The initial password is then entered by the infrastructure personnel, advising the user to set the new password complying with password restrictions.
- For existing employee, a self-service password reset solution that prompts a user with a series of customized questions is an effective approach to addressing password resets.

3. Force expiration of initial or “first-time” passwords

- User is issued a new account and not access that account for a period of time.
- As mentioned previously, initial passwords have a higher risk of being guessed or intercepted depending on what process is being used to create and distribute passwords.
- Forcing an initial password to expire after entering the password first time, helps mitigate this risk.

Liability:

Responsibilities

- The IT Service Management Steering Committee is responsible for reviewing and approving the policy and ensuring that it reflects the current requirements of SCAD.
- IS/IT Department to conduct a risk assessment against Internal policies and standards, and provide the approval based on the outcomes.

Prepared By Information Security Team	Reviewed By Director Information Security Office	Approved By Director Information Security Office	Released By Corporate Strategy & Excellence	Page 5 of 5
---	--	--	---	-------------