

## Table of Contents

|                                  |          |
|----------------------------------|----------|
| <b>1. Purpose .....</b>          | <b>3</b> |
| <b>2. Scope .....</b>            | <b>3</b> |
| <b>3. Compliance Table.....</b>  | <b>3</b> |
| <b>4. Responsibilities .....</b> | <b>3</b> |
| <b>5. Guidelines .....</b>       | <b>4</b> |
| <b>6. Enforcement .....</b>      | <b>6</b> |

## DOCUMENT CONTROL

### VERSION CONTROL

| Document Control ID | EFR-Password Policy-030                      |
|---------------------|----------------------------------------------|
| Issued Date         |                                              |
| Effective Date      |                                              |
| Owner               | Information Security & Compliance Department |

### REVISION TABLE

| Date       | Version | Brief Description     | Author              |
|------------|---------|-----------------------|---------------------|
| 04/11/2024 | 1.0     | Draft-Password Policy | Ms. Ratisha Kukreja |
| 03/12/2024 | 1.0     | Final-Password Policy | Ms. Ratisha Kukreja |

### RELEASE AUTHORIZATION

| Task        | Author              | Title      | Date |
|-------------|---------------------|------------|------|
| Prepared By | Ms. Ratisha Kukreja | Consultant |      |

### REVIEWER AUTHORIZATION

| Task        | Author                   | Title      | Date |
|-------------|--------------------------|------------|------|
| Reviewed By | Mr. Antony Arul Selvaraj | Consultant |      |

### APPROVAL AUTHORIZATION

| Name | Title | Signature | Date |
|------|-------|-----------|------|
|      |       |           |      |

**Important Note:** This document is intended solely for the use of the individual or entity to whom it is transmitted to and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

## 1. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

## 2. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any EFR facility, has access to the EFR network, or stores any non-public EFR information.

## 3. Compliance Table

| Policy/Procedure Name | ISO 27001:2022 Control | UAE IA Policy/Procedure Name | UAE IA Control | Requirements               |
|-----------------------|------------------------|------------------------------|----------------|----------------------------|
| Password Policy       | A.11.5.1               | Secure Log-on Procedure      | T5.5.1         | NIST SP800-144 Guidelines. |

## 4. Review

The policy shall be reviewed by EFR once a year, else whenever there is a change in the existing process.

## 5. Responsibilities

### General

- All system-level passwords and user-level passwords will be changed every 60 days.
- No default passwords shall be used on any appliance used within the network confines of EFR.
- System Level passwords are limited to:
  - Admin – Administrative Logins for Systems, Server and Network Monitoring Tool, Video Surveillance Tool.
  - Root access to Physical and Virtual Servers.
  - Access Point.
- User Level passwords are limited to:
  - Mail account
  - Workstation Login
- Password Complexity for all types of passwords in use within EFR premises, refer guidelines for basic complexity, as defined for the EFR network.
- Password Minimum Age for User-level & System-Level: 1 day.
- Password Maximum Age for User-Level & System-level - 90 days.

- Account lockout duration – 15 minutes.
- Account Lock Threshold for User Level & System Level - 5 (Five) Attempts.
- Password History for User Level & System Level - Last 10 (Ten).
- For User Level passwords, the system will prompt on every logon to change the password from the minimum password age day till the password is changed on or before the maximum password age day. Account will be locked, if this request is neglected.
- For all System Level passwords, passwords will be reset manually on or before the 60th day.
- User ID's will be unique. User ID will be communicated soon after Access Control into the work areas are created. The Password will be communicated to the corresponding employee in a secure manner through mail with a request to change the password within 30 minutes. Albeit the system will force the user to change their password immediately on Login. Password history for the last 10 passwords will be maintained.
- All default/ system passwords as set by manufacturers and / or vendors will be changed on installation / implementation.
- **Forgotten Password:** All users are required to maintain and protect their own account passwords. If a user has forgotten their password, they must contact the System Administrator during normal hours of operation to have the password reset.
- **Compromised Passwords:** If a password is suspected to have been compromised, the incident must be reported to the IT System Administrator and all passwords for the said user must immediately be revoked and suspended.
- **Password Resets:** Account access is terminated for users who are no longer in good standing / terminated / relieved from EFR, and passwords will be immediately changed by the System Administrator to prevent continued account access.
- All User Level and System Level passwords would conform to the guidelines described below.

## 6. Guidelines

### General Password Guidelines

- All users at EFR should be aware of how to select strong passwords:
- Strong passwords have the following characteristics:
  - Should contain at least 12 characters.
  - Should contain both upper- and lower-case characters (e.g., a-z, A-Z).
  - Should contain special characters (e.g., @\$%^&\*()\_+|~-=\`{}[]:~<>/ etc.).
  - Should have at least one Numeric character.
- Weak passwords have the following characteristics:
  - The password is a word found in a dictionary (English or foreign).

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- Try to create passwords that can be easily remembered.
- (NOTE: Neither of these examples are to be used as passwords).

### **Password Protection Standards**

If someone demands a password, refer them to this document or have them call someone in the

- Do not use the same password for EFR accounts and non-EFR access.
- Do not share EFR passwords with anyone, including administrative assistants or secretaries.
- All passwords are to be treated as sensitive, Confidential EFR information.
- Shall not store passwords in clear text or in any easily reversible form.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not hint at the format of a password.
- If someone demands a password, refer them to this document and direct them to the System Administrator.
- Always decline the use of the "Remember Password" feature of applications.

If an account or password is suspected to have been compromised, report the incident to the Information Security Risk Management team and change all passwords.

### **Application Development Standards**

Application developers must ensure their programs contain the following security precautions.

Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

### **EFR's Prescribed Password Characteristics**

Further subscribing to the fact that strong passwords are in effect a good practice to follow generally.

At EFR, we will follow the Strong Policy framework

- Passwords must have a minimum of 12 characters.
- Passwords must have both upper- and lower-case characters (e.g., a-z, A-Z).
- Passwords must contain special characters (e.g., @#\$%^&\*() \_+|~-=\`{}[]:~<>/ etc.).
- Passwords must contain at least one Numeric character.
- Password history up to 10 previous passwords will be stored, and an attempt to use a password already used within the 10, previous cycles will be disallowed.

## **7. Enforcement**

Any employee found to be violating this policy would be subject to disciplinary action, up to and including termination of employment.

**--End of Document--**