

Table of Contents

1. Purpose	4
2. Scope	4
3. Roles and Responsibilities	4
4. Compliance Table	4
5. Review	4
6. Principles	5
6.1 Need to Know	5
6.2 Least Privilege	5
6.3 Segregation of Access Control Roles	5
7. Procedures in Details	5
7.1 Security Requirements of Business Applications	5
7.2 User Access Management	5
7.2.1 Access Provisioning	6
7.2.2 Assigning User ID's	6
7.2.3 Access Provision to Vendors and Third Parties	7
7.2.4 Revocation of Access	7
7.3 Management of Privileged Access Rights	7
7.4 Access to Networks and Network Services	8
7.5 Management of Secret Authentication Information	9
7.6 System Access Control	10
7.6.1 Operating System Access Control/Access to System Utilities	10
7.6.2 Unattended User Equipment and System Time-Out	10
7.6.3 Secure Log-On Procedure	11
7.6.4 Use of Privileged/System Utility Programs	11
7.7 Enforcement	12
7.8 Emergency Procedures	12
8. User Responsibilities	12
8.1 General Procedures	12

8.2 Password Rules.....	13
9. Review of User Access Rights.....	13
10. Access Logs.....	14
Annexure A - Requisition for Creation of New Account (Email).....	15
Annexure B - Requisition for access rights for application systems	15

DOCUMENT CONTROL

VERSION CONTROL

Document Control ID	EFR-Access Control Policy-025
Issued Date	
Effective Date	
Owner	Information Security & Compliance Department

REVISION TABLE

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

Compliance with the Access Control Policy will enable EFR to minimize its exposure to any security breaches by ensuring users, systems administrators, technical support staff, and others utilizing EFR's resources, perform their activities within the framework established by law.

The objective of this procedure is to:

- Ensure authorized user access and prevent unauthorized access to systems and services.
- To make users accountable for safeguarding their authentication information.
- To prevent unauthorized access to systems and applications.

2. Scope

This policy covers access control for Physical and Logical access and is applicable to all EFR employees, merchants, contractors, and third-party users employed, contracted by EFR that have access to EFR assets, building premises, and information processing facilities.

3. Roles and Responsibilities

Asset owners – Shall determine appropriate access control rules, access rights, and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risk.

Data Owners – Will be responsible for defining and maintaining access control lists for applications and data.

Physical Access – Admin Team/Human Resource Team is responsible for ensuring the implementation of physical access control requirements. Users are responsible to adhere to the procedures as mentioned in this document.

Logical Access – Human Resource Team /IT Team is responsible for ensuring implementation of logical access controls across systems, IT devices, and applications, and access is to be provided on approval from Management. Users are responsible to ensure that the access provided to the information processing facilities and information/data are used strictly for business purposes only.

Management responsibility – All physical and logical access requests shall seek management's approval prior to granting access. Access provisioning for exceptional cases (esp. that involve risk to EFR and/or is not as per the access control policy) shall be granted only after the approval from Head of Operations.

4. Compliance Table

Policy/Procedure Name	ISO 27001:2022 Control	UAE IA Policy/Procedure Name	UAE IA Control	Requirements
Access Control Policy	A.11.1.1	Access Control Policy	T5.1.1	NIST SP800-144 Guidelines.

5. Review

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

6. Principles

EFR shall incorporate the below listed access control principles while granting access (physical or logical) to a staff/contractor/third party.

6.1 Need to Know

The 'need to know' principle shall apply to all users such that even if one has all the necessary official approvals, access to the information resources may be restricted to a minimum as required by the user based on the job role or business requirements.

EFR users will be granted access to information, data and applications based on their "Roles and responsibilities" and shall be granted certain access if and only if they are required to conduct one's official duties.

6.2 Least Privilege

A user or process shall be given no more access privilege than required. A principle of 'Least privilege' shall be achieved by limiting the resources that can be accessed as well as limiting the actions that can be performed by the user with authorized access to the resource.

6.3 Segregation of Access Control Roles

Segregation of access control roles (e.g., access request, access authorization, access administration) shall be considered to minimize incidents related to fraud, errors, and non-accountability of user actions.

7. Procedures in Details

7.1 Security Requirements of Business Applications

Accesses to applications shall be granted as per the requirements of the business. However, access shall be provided considering EFR's access control principles and including the access restriction requirements like:

- Providing menus to control access to application system functions.
- Controlling which data can be accessed by a particular user.
- Controlling the access rights of users, e.g., read, write, delete, and execute.
- Controlling the access rights of other applications.
- Limiting the information contained in outputs.
- Providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

7.2 User Access Management

- All EFR system components shall be covered by the access control system.
- EFR users will be granted access to information, data, and applications on a "need to know" basis. Access will be restricted according to the user's requirement to access information, data, or application based on the least privilege to achieve the desired business function. 4

- Users will be defined only once to a particular application.
- Accesses shall be provisioned after obtaining approval from the owner of the information system or service for the use of the information system or service and separately from management may also be appropriate.
- For all information classified as public, users will be allowed an 'enquiry' facility to such information. Users will not be allowed to modify such data unless authorized.

7.2.1 Access Provisioning

- Respective department leads/heads shall raise the request for new id creation to Department Head/Data Owner/designate for approval. User access rights to applications and data will be established and maintained by the relevant System Administrator on receipt of an approved written request only.
- All access requests will include the reason why access is being requested and a written approval provided by the Data Owner or designate.
- Authorization form or tickets shall be used for all access provision, modification, or removal. The authorization form shall specify the required privileges and shall be approved by the concerned manager.
- The Data Owners will ensure that the level of access granted is appropriate to the EFR's purposes and is consistent with other requirements such as segregation of duties.
- Authorized changes to user access rights will be made promptly by the relevant System Administrator. System access rights will be revoked prior to or as soon as possible after personnel leave the EFR.
- A central record of access rights granted to a user ID to access information systems and services shall be maintained.

7.2.2 Assigning User ID's

- Access to information services will be controlled by using unique User Ids so that users can be linked to and made responsible for their actions. *
- There will be a one-to-one relationship between user Ids and individuals. Users shall use a unique username and password for logging into EFR's systems, which will be authenticated through google authenticator.
- Administrator accounts shall also have unique user ids.
- User Ids will follow a standard naming convention for all computer systems to facilitate user identification. Naming conventions will cover all end users, contractors, consultants, auditors, and vendors.
- All user accounts created in computer systems will have an applicable, informative full name and description.
- Users ID along with default password shall be shared by the parameter with users and users are required to change the password in first login.

- Unique user IDs shall be assigned to every user to enable users to be linked to and held responsible for their actions.
- The use of shared IDs shall only be permitted where they are necessary for business or operational reasons and should be approved and documented.
- Temporary user ids shall be created with proper approval of the Function-head and Head of IT for a limited period. These will be reviewed on a regular basis and access rights will be revoked when no longer required.

7.2.3 Access Provision to Vendors and Third Parties

- Physical access shall be provided to the vendors, on the signing of a visitor pass by the vendor. All vendors shall be escorted by employees concerned to the relevant area of work and will be monitored while on the premises.
- Data center physical access requests shall be approved by the Datacenter – in charge prior to providing entry.
- Information Systems shall be provided to any vendor/supplier on approval from the Head of IT.
- Third parties are provided with accounts that solely provide access to the systems and/or data they are contracted to handle, in accordance with the least privilege and need to know principles and/or approval from the Head of IT. The accounts will be removed at the end of the contract or when no longer required.
- Unless operationally necessary (and explicitly recorded in the system documentation as such) third-party accounts will be disabled when not in use.

7.2.4 Revocation of Access

- If a person no longer requires the level of access he has been granted, the Data Owner /Department Head/designate will inform the same in writing to the relevant System Administrator with a copy to the Administrative, so that it can be revoked.
- Immediately after a staff/vendor/third parties leave the team/process/EFR, all the physical and logical accesses (user accounts, email IDs, access to servers, network devices, etc.) of that staff/vendor shall be appropriately disabled.
- The Head of IT shall block the user id (for all critical applications) in all the above cases. At the end of every month, the parameter team shall disable the IDs from the system.
- Access rights shall be immediately reduced or removed in case of a serious information security breach.
- If a user account has been inactive for more than 60 days, the system should automatically deactivate the user, or the system manager should manually suspend it.

7.3 Management of Privileged Access Rights

- The allocation of privileged access rights shall be controlled through a formal authorization process. User IDs with special system privileges will be controlled and restricted to a limited number of authorized personnel. These will include IDs, which are used to administer modifications to the operating system, security functions, and audit logs.

- Privileged access rights should be allocated to users on a need-to-use basis and on an event-by-event basis.
- An authorization process and a record of all privileges allocated should be maintained. Privileged access rights should not be granted until the authorization process is complete.
- Generic administrative accounts shall be limited as much as possible, and records of approvals and justification of maintaining such accounts shall be retained. Privileged User IDs like system administration accounts will not be shared by more than two users who require this level of access to perform their job duties.
- Regular business activities shall not be performed from privileged ID. Privileged access rights shall be assigned to a user ID different from those used for regular business activities.
- A record of all privileges allocated shall be maintained and the competences of users with privileged access rights should be reviewed regularly. Changes to privileged accounts should be logged for monthly periodic review.
- System Administrator will logon as themselves, using a normal User ID when performing regular work duties rather than logging in as the Supervisor/Administrator. Logging in as the Supervisor/Administrator will be limited to administrative activities only. Guest accounts or related features (where applicable) will be disabled wherever applicable.

7.4 Access to Networks and Network Services

To prevent unauthorized access to network services, EFR shall:

- Provide network access, to users, only to the services that they have been specifically authorized to use.
- Enforce appropriate authentication methods, by subjecting users to strong authentication (Two factors) route traffic through firewalls and limit the methods of connection, to manage and control access by remote users. External connections should be individually identified, verified, recorded, and approved.
- Ensure that all diagnostic and configuration ports shall be adequately protected, through logical and physical access controls. This would ensure that Physical security for on-site diagnostic and configuration ports, technical security for remote diagnostic and configuration ports, disabling/removing ports, services, and similar facilities which are not required for business functionality are addressed.
- Put in place different network segments and network segregation based on functional groups. Physical/Logical segregation of the network will be performed on a requirement basis.
- Segregation of networks shall comprise and address groups of information services, users, and information systems.
- Restrict the capability of users to connect to the network, especially those extending across EFR's boundaries, based on the individual's roles and required level of the capability ability of users to access the network would be restricted by Access Control lists.
- Implement Routing controls to positively check the source and destination address and where required limit the route between the user terminal and the computer services that, the user is required to access.

- Users will be limited to a single concurrent session on all networked computer systems unless approved in writing by the immediate controlling authority.

7.5 Management of Secret Authentication Information

- A password expiration period of 2 months will be set, so that users are forced to change their passwords accordingly.
- Passwords will never be displayed in clear text or stored in readable form in batch files in automatic login scripts, in terminal function keys, in computers without access control, or in other locations where unauthorized people might discover them.
- The use of masking or character suppression features will always be employed for system and application logon routines.
- Users shall be provided initially with secure temporary secret authentication information for the first time. The provisioning of the temporary secret authentication information shall be done in a secure manner. The temporary secret authentication shall be unique to an individual and should not be guessable. The users shall acknowledge receipt of secret authentication information.
- The system or application shall force the user to change the password (issued by the System Administrator) at the time of the initial logon, wherever possible.
- Default passwords, shipped with software upon installation of the software or receipt of a system with pre-loaded software, will be immediately changed.
- The practice of "recycling" or reusing the same password when prompted for a change will be prevented, where possible. A history of last 10 passwords will be retained or users will not be allowed to reuse passwords within a period of 10 months, wherever practical.
- Group passwords will be disallowed to maintain individual accountability, unless approved in writing by the immediate controlling authority.
- System Administrator will convey temporary passwords to users in a secure manner. Conveyance of passwords through unprotected (clear text) electronic mail messages will be avoided. The initial passwords created will conform to the password construction procedures, difficult to guess, and unique to each user.
- Passwords will not be included in any automated logon process. Exceptions to this procedure will be brought to the notice of the immediate controlling authority.
- Authentication codes/passwords transmitted across the network will be encrypted.
- A trusted version of the operating system will be reloaded, wherever possible to prevent easier cracking of passwords by password cracking programs.
- The User ID and password for highly privileged users e.g., Supervisor/Administrator will be stored in a sealed envelope and placed in a secure location under custody of the Administrative. The Administrative will ensure that an authorized employee has access to this password if the System Administrator cannot be reached during an emergency. The use of this password will be logged, and the password will be changed immediately after use.
- In the event a staff member who has privileged access is terminated or has resigned; the password for privileged access will be changed on the same day. The administrative is responsible for ensuring that the password is changed on the same day.

- System master passwords if available and used, will be restricted to, and maintained by, the Administrative.
- System files holding authentication data or passwords will be protected from unauthorized access.
- All users will sign an undertaking to keep passwords confidential and acknowledge liability for transactions done using their passwords.

7.6 System Access Control

7.6.1 Operating System Access Control/Access to System Utilities

To prevent unauthorized access to operating systems, EFR shall:

- Put in place operating systems secure log-on procedures, to restrict access only to authorized users by enforcing strong authentication procedures.
- Require that users have a unique identifier (user ID) and use strong authentication techniques. Users' identity will be substantiated and verified, and if required identify the terminal or location of the user.
- Use password management systems that ensure use of quality passwords and provide reasonable level of protection of stored passwords.
- Put in place hardening procedures for operating system, applications and firmware installed on network devices (routers and firewalls) thus enabling the services that are required to run, for performing the business operations and activities.
- The folders or disk drives in individual PC's or laptops will not be shared unless share level access controls have been enabled on the folder or the disk drive. All PCs and laptops containing Secret classes of information or data will not have any shared folders.
- Any removable media devices, such as CD Writers will not be added to individual PCs or laptops unless authorized and documented by the immediate controlling authority and Head of IT.

7.6.2 Unattended User Equipment and System Time-Out

- All systems and applications shall be configured to invoke time-out facilities that automatically log-off workstations/applications after a set period of inactivity, clear screens and require users to sign-on again before restoration of screens. The sensitive applications should require use of a hardware-based token in addition to password entry for re-authentication.
- All users will terminate their active sessions, when finished, unless they can be secured by an appropriate locking mechanism (e.g., re-authentication of user etc.)
- In the case of Secret classes of information or data, users will always terminate their active session and secure the PC or laptop when leaving it unattended.
- Password protected screensavers will be used to protect user terminals wherever applicable when left unattended. A standard screensaver will be used across EFR, and users are prohibited from installing a screen saver other than the approved standard screen saver. The screensaver will be activated within a time frame of 5 minutes of inactivity.

7.6.3 Secure Log-On Procedure

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens, or biometric means, shall be used.

EFR shall ensure that their log on procedure shall:

- Not display system or application identifiers until the log-on process has been successfully completed.
- Prior login, a legal login banner shall display a general notice warning that the computer should only be accessed by authorized users.
- Not providing help messages during the log-on procedure that would aid an unauthorized user.
- Validate the log-on information only on completion of all input data.
- Protect against brute force log-on attempts.
- Log unsuccessful and successful attempts.
- Raise a security event if a potential attempt or successful breach of log-on controls is detected.
- Transmitting passwords in clear text over a network is prohibited.
- Restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

7.6.4 Use of Privileged/System Utility Programs

- All system utilities which may be used to alter information, data or software will be identified and inventoried by the relevant System Administrator.
- The use of utility programs that might be capable of overriding system and application controls shall be restricted to authorized personnel in accordance with their business functions.
- Utility programs shall not be available to users who have access to applications on systems where segregation of duties is required. Application users will be restricted from accessing data directly via third-party tools or sensitive system utilities like SQL.
- Systems Administrator should ensure that normal users do not have access rights to use SQL like utilities and any backend level update to the data using SQL / similar utilities is done only after prior written approval from the IT Department.
- The use of sensitive utilities will be logged in "tamper-proof" logs by the Systems Administrator for review by auditors, wherever possible. The audit log and issues related to the usage of sensitive privileges/utilities will be reviewed on a regular basis and followed up for any inappropriate usage.
- Through a periodic compliance check, all unnecessary utility programs shall be removed or disabled.

7.7 Enforcement

In circumstances where an event is assessed to be a breach of the policy or standards of acceptable use, as described in this policy, or considered to be inconsistent with the ownership rights, such cases shall be monitored and investigated.

Violation of the provisions of this policy and its components shall be liable for following actions:

- Disciplinary action and can extend to legal action.
- The subject alleged with the violation and the events triggered by them shall be subject to investigation.
- Subject to the findings of any such investigation, non-compliance with the provisions of the policy could lead to appropriate disciplinary and legal action, that could include but not limited to dismissal of the user, termination of contract thereof, etc.

7.8 Emergency Procedures

Emergency ids with high-level access privileges will only be used in the event of extreme emergency*.

Passwords of Emergency IDs will be stored securely under the custody of the Departmental In-Charge will ensure that an authorized employee has access to this password if the System Administrator cannot be reached during an emergency*.

All emergency actions, which bypass normal access control procedures, will be logged, and reported to the Head of IT for immediate review. *

Resource or designated owners will be notified immediately of all emergency fixes, and they will retrospectively review all emergency amendments.

8. User Responsibilities

8.1 General Procedures

- Nobody should use another user's ID to gain access to computer resources. *
- Default user file permissions must not allow anyone other than the owner of the file to read, write, and/or execute that file. Users may reset permissions on a file-by-file basis if access to these files must be granted to other users. Word writeable files must be kept to a minimum.
- The users will periodically delete from the local hard disk any confidential information that is no longer needed or move it to a secure location on the server. *
- Unauthorized software will not be installed on individual PCs or laptops. This includes but is not limited to the shareware, remote-access software, dial-out applications, and internet access applications. *
- Users will enable automatic screen blanking or activation of a screen saver feature after 5 minutes of inactivity, wherever possible.
- Users will note the last login time and date while logging into the system time to ensure that an unauthorized person has not used their user ID.

8.2 Password Rules

- The minimum length of passwords will be set as 14. It should contain alphabets, alphanumeric and special characters.
- The password also will not contain consecutive identical characters or all-numeric or all-alphabetical groups.
- The passwords will not be based on anything that somebody else could easily guess or obtain using collateral information (e.g. names, telephone numbers and dates of birth etc.) like: *
 - Passwords relating to one's personal life
 - Common words found in dictionary
 - Technical words relating to the EFR's computer systems environment
 - Famous dates
 - Passwords relating to one's personal life in reversed order
 - Prominent individuals
 - Same as the user's login name (sensitive or insensitive case) or a reverse shift of the login name.
- In the case of Secret classes of information or data, users will choose passwords that are a minimum of 14 characters in length. *
- Users will never share or divulge their passwords. *
- Users will input all passwords themselves, when receiving technical assistance. *
- Users will promptly change passwords that have been compromised or are suspected of being compromised. *
- Users will change their password monthly. *
- Users will select new passwords when existing passwords have expired. The practice of "recycling" or reusing the same password when prompted for a change is expressly prohibited wherever possible*.
- Passwords will not be stored in readable format in batch files, log-in scripts, terminal function keys, files on local hard drives, "stickers" or any other locations where authorized / unauthorized persons might discover them*.
- Users will not use any software "password-remember" features (in any application/system) which would defeat the purpose of having the software require a password for authorization purposes*.
- Passwords set by the System Administrator when defining users to systems or resetting an existing password will be changed immediately by the rightful password owner. *

9. Review of User Access Rights

Access rights shall be reviewed periodically **every month** for the users and the special privileged access rights shall also be reviewed **monthly** to identify and remove or disable redundant user IDs. System Administrators

should verify the active users of any application to weed out and inactive / delete User IDs, which are no longer needed. This shall be accomplished by periodically reviewing access rights with owners of the information systems or services.

The Data Owners/Department Head/designate shall review users' access rights at regular intervals of a month-on-month basis and after any changes, such as promotion, demotion, and change in role, transfer, or termination of employment for identifying inactive accounts or accounts that would be inactive for several reasons like approved medical leave, official tour, etc. The Data Owners will inform the System Administrator in writing to disable such accounts.

Users' access rights will be reviewed periodically by **the 15th of every month.**

Authorizations for special privileged access rights will be reviewed every month.

10. Access Logs

- All-access violation attempts (user and resource authentication) will be logged and reported by the Systems Administrator to the Department In-Charge as deemed appropriate.
- Access violation logs will be reviewed daily by the Systems Administrator and reported to the Department In-Charge so that action plans can be initiated to prevent their recurrence.
- All system and application logs will be maintained in a form that cannot readily be viewed by unauthorized persons. A person is unauthorized if he or she:
 - Is not a member of internal audit staff
 - Is not a member of systems security staff
 - Is not a member of systems management staff
 - Does not need to have such access to perform regular duties
- Hard copies / Printed versions of logs containing events of access violation should be separately preserved as evidence and mailed to the Information Security Risk Management Team and Head of IT.

Physical Access Request Form:

Annexure A - Requisition for Creation of New Account (Email)

Requisition for Creation of New Account	
Name of the user:	Date:
UAT/Prod:	Department:
Application Systems and Data files	
Other OS Privileges(e.g., SFTP, remote login etc)	
Requisitioned by:	

Authorization:

Grant the following access to the user
Revoke the following rights/privileges to the user
Authorized by:
Date:

For Official Use Only:

Access granted to the user:	
Access revoked for the user:	
User ID created:	
Performed by:	Date:

Annexure B - Requisition for access rights for application systems

Requisition for access rights for Application Systems	
Unit:	Date:
Name of the user:	Department:
Application System:	
Menu Options:	
Database access rights:	
Requisitioned by:	

Authorization:

Grant/modify the following access rights to the user
Revoke the following rights/ privileges to the user
Authorized by:
Date:

For Office Use Only:

Access granted to the user:	
Access revoked for the user:	
User ID created:	
User ID Revoked:	
Email Id Revoked:	
Performed by:	Date:

--End of Document--