

Table of Contents

1. Purpose	3
2. Scope	3
3. Definition of Change	3
4. Roles and Responsibilities	3
5. Compliance Table	4
6. Review	4
7. Procedure	4
7.1 Initial user request	4
7.2 Change Assessment	4
7.3 Priority	4
7.4 Change Authorization	5
7.5 Change Testing	5
7.5.1 Unit testing's	5
7.5.2 Integration testing	5
7.5.3 User and System Acceptance Testing	6
7.6 Implementation	6
7.7 Fall back	6
7.8 Documentation	6
8. Change Control Review and Monitoring	7
Annexure	7

DOCUMENT CONTROL

VERSION CONTROL

Document Control ID	EFR-Change Management Procedure--015
Issued Date	
Effective Date	
Owner	Information Security & Compliance Department

REVISION TABLE

Date	Version	Brief Description	Author

RELEASE AUTHORIZATION

Task	Author	Title	Date

REVIEWER AUTHORIZATION

Task	Author	Title	Date

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

Inadequate control of changes to information processing facilities is a common cause of system or security failure. To minimize such system or security failure, all system updates will be properly controlled and managed. The implementation of change management and control strategies will help to mitigate risks such as:

- Information being corrupted and/or destroyed;
- Computer performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Exposure to reputational risk.

2. Scope

Any EFR user including employees, third party users, who need to request or implement a change to any element, needs to abide by this procedure.

Formal management responsibilities and procedures will be in place to ensure satisfactory control of all changes to hardware, software (application, OS) or procedures.

3. Definition of Change

In terms of these Change Management Procedures, a change is defined as the addition of any item to, the deletion of any item from, or the alteration of any item of EFR.

For the purposes of these procedures, changes are defined in terms of three categories namely:

- A change which relates to the development of a new program, or which alters the functional characteristics of an existing program.
- A change, which is to fix a fault with the operation of an existing program. This type of change is required to make the program conform to the most relevant, approved functional specification.
- Changes, which are of an operational/housekeeping status, typically implemented during normal day-to-day market operations, and this type of change, are managed differently to other changes.

4. Roles and Responsibilities

The following are criteria by which the Change Management Process can be evaluated:

1. The team leaders and process owners shall initially approve the requests as per the business requirements.
2. The Information Security Risk Management Team shall establish the security requirements for the changes and assess the risks associated with the changes.
3. Head of Engineering shall approve the implementation of the change. Management shall take a final decision in case the changes deviate from the EFR's security policies and standards.

5. Compliance Table

Policy/Procedure Name	ISO 27001:2022 Control	UAE IA Control Policy/Procedure	UAE IA Control Number	Requirements
Change Management Procedure	A.10.1.2	Change Management	T3.2.3	NIST SP800-144 Guidelines

6. Review

The review of this procedure is done on an annual basis or in case there is a significant change in the existing procedures.

7. Procedure

7.1 Initial user request

In case the user requires any amendments to an application program, the user must submit his requirements through the mail or through Change Request Form to the Head of Engineering. The requirements should come from the Department head.

The requirements could relate to bugs in the existing functionality, frequent error messages indicating that some parts of the programs are incorrect, additional features required to be built in the system or report customization.

7.2 Change Assessment

The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable, consider compliance with legislative requirements and standards.

The assessment shall consider the business as well as security impacts associated with the change.

7.3 Priority

The term priority is used to indicate an urgency and / or timeframe expected in response to a change request.

Four levels of priority are defined which are:

1. Urgent

An acute error in EFR information system causing shutdown or failure or unsatisfactory operation is treated with urgent priority.

2. High Priority

A serious error in EFR information system that interferes with the operation of the system but does not actually prevent its use or operation is treated with high priority.

3. Medium Priority

An error in EFR information system where alternative solutions is available that is acceptable temporarily is treated with medium priority.

4. Low Priority

Imperfections in the use of TechOps based screens, help text, documentation or improvements or suggestions to Ops facilities that have no significant effect on the use or operation of EFR information system are treated with low priority.

7.4 Change Authorization

- All changes should be approved and effected based on formal change requests.
- Change requests should be approved by the Data Owner considering the business justification of the request while the Head of Technical Team will determine if the request is technically feasible.
- If the change request involves incorporating data from a different application, the Data Owner of that application will also need to approve the request.
- Only approved change requests shall be implemented and processed.
- Status of the Change (along with dates) may be maintained with following fields Status
 - Initial discussion
 - Impact Analysis
 - Approved for Implementation
 - Work in Progress
 - Change Testing
 - Implemented
 - Rolled Back
- Approval for implementing the changes shall be provided by the Head of Engineering.

7.5 Change Testing

Before adapting to any new software / program, it should be tested in the quality server.
Following testing methods are adapted:

7.5.1 Unit testing's

The unit tests then allow the location of the fault or failure to be easily traced. When the unit tests pass, that software/ program is considered complete. If the unit tests fail, it is a bug either in the changed software/ program or the tests themselves.

Unit testing is carried out to find any errors in development and design and their test results should be documented indicating the deviation, test cases carried out and gaps found if any.

The developers / peers will conduct unit testing in the programmer's development library. The developer's manager will perform an independent review of unit test results.

Sanitized copies of production data or dummy data sets will be used for testing purposes.

7.5.2 Integration testing

The purpose of integration testing is to verify functional, performance, and reliability requirements placed on major design items. Test cases are constructed to test whether all the components within assemblages interact correctly. Integration testing is carried out in new systems to protect the designs from malfunctioning.

All significant modifications, major enhancements and new systems will undergo integration testing prior to implementation of the change in production. For major enhancements and new systems, a formal integration test plan will be prepared.

Integration testing will be conducted in a separate, independently controlled test environment. If problems are noted, then the developer will make appropriate modifications and submit it to release engineer for re-testing.

Sanitized copies of production data or dummy data sets will be used for testing purposes.

Integration test results will be documented and kept on file.

7.5.3 User and System Acceptance Testing

All significant modifications, major enhancements and new systems will be tested by appropriate end users prior to installation of the software in production.

User acceptance testing will be conducted in a separate, independently controlled test environment.

For major enhancements and new systems, a formal user acceptance plan will be prepared. The plan will include tests of all major functions, processes and interfacing systems.

Requesters will indicate acceptance through a formal sign-off.

During acceptance testing, logical access restrictions will ensure that developers have no update access and that the code being tested cannot be modified without the written consent of the user.

7.6 Implementation

Implementation will only be undertaken after appropriate testing and approval by management. All major changes shall be treated as new system implementation and shall be established as a project.

The process owner or the designate will communicate with all relevant users affected by the changes about the change details.

7.7 Fall back

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert to what they were prior to implementation of changes.

7.8 Documentation

The change management process will involve recording and managing the documented change requests for system modifications.

The change requests will provide a brief description of the changes requested, the date on which the request was made, prioritizing the request, tracking and controlling modifications and assigning a unique number to each request.

Change requests will be chronologically documented for different applications with each request identifiable with a unique number to facilitate easy reference and tracking.

- Details on the changes established shall be retained for future reference.
- Test reports shall include the scope of testing, results and test cases considered.
- Information resources documentation shall be updated on the completion of each change and old documentation shall be disposed of as per the media disposal procedures.
- Policies and procedures, affected by software changes, shall be updated on completion of each change.

8. Change Control Review and Monitoring

- As per the status of the changes maintained, there shall be periodic discussion from all process owners related to the issues faced during implementation of the change. The discussions shall be documented along with the corrective actions taken for the discussed issues.
- The effectiveness of change management process can be evaluated by maintaining Management reports. The reports may include the number of successful and unsuccessful changes per month, by category, by source and by trends. The report will also provide an analysis of the unsuccessful changes, together with a statement of the effects of the failures.
- All change requests will be monitored for their Implementation Status viz. Accepted and Implemented, Work in Progress, deferred till dd/mm/yy for implementation and rejected.

Annexure

Change Authorization Format

General Information	
Project Name	Date
Details of Change requested	
Description – Describe the proposed change.	
Change initiated by	
Name of the official who approved the change both from business side and IT side(If change initiated by other departments, provide supporting document)	
Reason for changes	
Impact of Not Implementing – Explain the impact if the proposed change is not implemented.	

Impact on overall Information security posture and controls implemented

Change Request Analysis

Impact Description – Describe the impact for each of the items checked.

☐ Configuration Item

If Hardware - Details

If software – details

☐ Estimated Project Schedule

Change request ID

Change Request Final Management Approval

Signature :

Final Approval Date

Name

Title

Recommendation

☐ Approve ☐ Reject

Special Instructions – Provide any additional information regarding the final recommendation.

Change request follow up:

Project completion details:

Change request ID

Program Name

Date of receipt of modified program

Dependency on other modules/Other modules getting effected

Tested by

Test results recorded (PI attach copy of recordings of test result)

Patch No:

Movement to production authorized by

Project completion details:	
Date of Porting to production	Ported By
Version of Application:	
Before implementation:	After implementation:
Whether back up of existing version taken and required fallback arrangements: (Provide Date of back up)	
Any other details	

--End of Document--