	Document Title	Document Number	Issue Date
سدرة للطب Sidra Medicine	**IT CHANGE MANAGEMENT**	**536**	**21/04/2016**
	Approved By	**Version Number**	**Review Due Date**
POLICY	**Executive Director – Information Technology**	**1**	**26/05/2023**

If you print this document from the Electronic Manual, the copy is valid only until midnight of the day you printed it.

SCOPE	Organizational ☐ Departmental ☒
TITLE	IT Change Management
PURPOSE	Establish the rules for managing IT systems and applications changes in a controlled manner to minimize errors, risks, productivity losses, performance disruptions, information corruption and unauthorized changes on the systems.
APPLICABLE TO	Information processing systems, applications and servers used by the authorized Sidra IT staff, vendors and third party contractors.
DEFINITIONS	**Change Request** (CR) - A formal proposal for an alteration to a system or an application or information asset. **Change Management** - The process for controlling the lifecycle of all changes. The primary objective of Change Management is to enable changes to be made, with minimum disruption to services; to reduce the risks posed by changes to the information processing environment and to improve the reliability of the processing environment as changes are made. **Normal Change** - A Normal Change to a system that must be assessed planned, tested, coordinated, communicated and approved by the CAB. **Emergency Change** - A change performed as an immediate response to a service interruption that is classed as high impact, either on account of the number of users affected or because systems or services that are critical to the organization are involved. **Standard Change** - A Change that is recurrent, well known, has a documented procedure (SOP), relatively risk-free path, and is the accepted response to a specific requirement or set of circumstances, where authority is effectively given in advance of implementation. Also known as Pre-Approved Change. **Change Advisory Board** (CAB) - A group that advises the Change Manager in the assessment, prioritization and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, the Business and Third Parties. CAB decisions are made through consensus. **Emergency CAB** (eCAB) - A sub group of available CAB members, Change Manager, Coordinator, Change Initiator, Business and Technical Managers who will review emergency Change Request in an event when CAB is not scheduled to review Change Request in timely fashion
EXPECTED OUTCOME	Implement a Change Management process to ensure proper assessment, control and

	authorization of all systems and applications implemented in the production environment.

POLICY STATEMENT

1. GENERAL STATEMENTS

1.1 The organization shall follow a disciplined process to introduce changes into its IT infrastructure and applications, with minimal disruption to ongoing operations.

1.2 Change Management shall be organized around the following activities:

1.2.1 Establish a common approach for requesting and documenting Change Requests;

1.2.2 Implement proper controls and authorizations for all Change Requests;

1.2.3 Describe the required communications or coordination points for properly processing changes; and

1.2.4 Create an audit trail of all organization's systems and applications Change Requests (CRs) including status of CR (initiated, tested, approved or implemented).

1.3 This policy shall be followed by all Sidra departments, vendors and third parties contractors requesting changes to or within the organization's IT Infrastructure and applications (Production, Training, Test, Build & Disaster Recovery, and others) including, but are not limited to changes such as:

- Application changes
- Interface changes
- Application version upgrades, enhancements, or patches
- Planned outages
- System software / configuration changes
- Database changes
- Network changes
- Hardware changes

2. CHANGE MANAGEMENT

2.1 No information asset that is critical or essential to the organization's operations or processes, that forms a part of, is connected to, or is hosted by the enterprise network, shall have its system or security baseline changed, be physically or logically moved, or be re-configured in any way, without following the approved Change Management procedure.

2.2 Authorized IT personnel shall configure all critical information assets, including the network, applications, services, or information systems, to provide only essential capabilities and shall specifically prohibit or restrict the use of specified functions, ports, protocols, and services.

2.3 All changes shall be assessed, authorized and planned before being applied to production.

2.4 All Changes shall be tested where applicable and possible.

2.5 A rollback procedure shall be documented before applying the changes.

2.6 All changes shall be assessed for their potential impacts and risks.

2.7 All systems that require amendment shall be identified before making a change.

2.8 Change Requests submitted for approval shall include sufficient testing documentation along with business approval.

2.9 All system documentation shall be updated on the completion of each change and the archived change documentation must be centralized.

2.10 Formal approval shall be obtained from the Change Advisory Board (CAB) for all proposed changes before implementation.

2.11 Only Emergency Changes can by-pass the Change Advisory Board approval process.

2.12 Emergency Changes are exceptional by nature. Emergency Changes shall be justified and approved by the system owner. All activities and documentation required for a normal CR shall be provided post implementation.

2.13 The Change Requester and / or the impacted user shall be notified about changes approval and implementation status.

2.14 The change advisory board permanent and temporary membership and frequency of meetings shall be defined as part of the Change Management Procedure.

2.15 A post implementation review shall be undertaken after CRs implementation and presented to the CAB when necessary.

3. ROLES AND RESPONSABILITIES

3.1 For any change, roles and responsibilities must be organized around the following functions:

Role	Responsibilities
Change Requestor [Business Member, IT Operations Member, Project	• Initiate a request for change • Modify a Change Request

Managers, Administrators]	• Provide / validate test scenarios • Approve test results
Change Manager (CM) [Change Control Officer]	• Monitor all change activities for an all environment within the Change Management Scope • Receive request for change from Change Requestors • Ensure all Change Requests supporting documentation is provided prior to CAB review • Tracks changes to closure • Receive, logs and allocates a priority, in collaboration with the requestor • Update the Change Control Log with all progress, including any actions taken to correct problems and/or to take opportunities to improve service quality • Review all implemented Changes to ensure that they have met their objectives. Refers back any changes that have been backed out or have failed • Close requests • Produce reports on agreed KPIs or metrics.
Change Advisory Board (CAB)	• Analyze the Change Request for validity, feasibility • Approve or Rejects changes implementation • Provide recommendations for improvement of Change Management control
Emergency Change Advisory Board (eCAB)	• Analyze the Emergency Change Request for validity, feasibility • Approve or Reject Emergency Changes implementation
Change Reviewer [Business Head, Specialists or Experts in Area]	• Review requested changes • Assess the impact of implementing the requested change • Assess resources and timing requirements for the change • The change reviewer must be a specialist / expert member in the area of change.
Change Implementers [IT Operations]	• Implement the approved change as requested • Provide status of change implementation. • Back out / roll back failed changes

COMPLIANCE REFERENCES	**1. ISO 27001:2013 Standard** 1.1 Change Management (A.12.1.2) 1.2 Controls against malware Protection of log information (A.12.2.1) 1.3 Management of technical vulnerabilities (A.12.6.1) **2. NIA Policy v2.0** 2.1 Governance Structure [IG] – Section 1.2 2.2 Change Management [CM] – Section 5.2 **3. ITIL V3 Service Transition** 3.1 Change Management (4.2)
RELATED DOCUMENTS	
REFERENCES	1. International Organization for Standardization (ISO). BS ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems – Requirements. ISO/IEC resources; 2013. 2. Ministry of Information & Communication Technology. National Information Assurance Policy v2.0. ICT Qatar resources; 2014.

NAME OF AUTHOR	Naoufal Rihani, Head - Information Security and Identity Management
POLICY OWNER/ DEPARTMENT	Executive Director – Information Technology / Information Management
APPROVAL BODY	As per POL - O - Tables of Decision Authorities (ToDA) and Financial Authorities (ToFA)
MEASUREMENT OF COMPLIANCE	Periodic Security Audits Annual Effectiveness Review
KEYWORD SELECTION	Keyword 1 : Change Keyword 2 : Control Keyword 3 : Emergency Keyword 4 : Change Advisory Board

Version Number	Issue Date	Summary of amendments Key Changes	Communication Message
1	21/04/2016	1.1 New document 1.2 May 2021. Reviewed by the author as current and relevant, no amendments required to this document at this time of review. Renewal without change approved by Abdulrahman Hasna on behalf of S Bhasker, Executive Director – Information Management. Next review due date extended to 26/05/2023.	