	Document Title	Document Number	Issue Date
سدرة للطب Sidra Medicine	**CYBER SECURITY MANAGEMENT REVIEW**	**297**	**13/11/2019**
	Approved By	**Version Number**	**Review Due Date**
POLICY	**Mohammed Khalid Al Mana – Chair, Transition Committee**	**2**	**13/11/2021**

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	Cyber Security Management Review
PURPOSE	To ensure that the security policies, procedures and other key components of the cyber security management system (CSMS) framework are reviewed at planned intervals, or if significant changes occur to ensure the suitability, adequacy, and effectiveness.
APPLICABLE TO	All Sidra staff with access to the organization's information or who have been granted access to systems or applications.
DEFINITIONS	**Corrective and Preventive Action (CAPA)** - consists of improvements to an organization's processes taken to eliminate causes of non-conformities or other undesirable situations. It is usually a set of actions that certain standards, laws or regulations require an organization to take in documentation, procedures, or systems to rectify and eliminate recurring nonperformance. CAPA is used to bring about improvements to an organization's processes, and is often undertaken to eliminate causes of non-conformities or other undesirable situations.
EXPECTED OUTCOME	A documented periodic review of information security policies, procedure and the effectiveness measurement of the CSMS.

POLICY STATEMENT

1. REVIEW CYCLE

1.1. The security policies developed by the Enterprise Cyber Security and Governance shall be reviewed every two years and at a minimum include the following:

1.1.1. Security Policy effectiveness.

1.1.2. Impact assessment of security controls on business and clinical operations.

1.1.3. Assessment of new technologies introduced into the organization

1.1.4. Proposals for implementing new security control.

1.2. In addition to the above, the security policies are subject to revision as a result due to a CAPA or observations made by the auditors, with or without prior notice.

1.3. As soon as a policy revision and approval provided by the authorized level of management, the Communications Department shall send notification to the Sidra staff that the policy has been revised.

2. REVIEW ENFORCEMENT

2.1. The organization's approach to managing cyber security and its implementation (i.e. control objectives, controls, policies, processes and procedures for cyber security) shall be reviewed independently at planned intervals or when significant changes occur.

2.2. Information systems shall be regularly reviewed for compliance with the organization's security policies and standards.

2.3. All security policies shall have a designated owner, who has approved management responsibility for the development, review, and evaluation of the security policies.

2.4. The periodic review of the security policies shall take into account the results of management reviews.

2.5. Inputs for the management review shall include information on:

2.5.1. Review of control objectives and controls

2.5.2. Feedback from the interested parties.

2.5.3. Results of independent reviews, which may be internal or external audits.

2.5.4. Status of preventive and corrective actions.

2.5.5. Process performance and information security compliance.

2.5.6. Results of previous management reviews

2.5.7. Results of actions taken to address security risks.

2.5.8. Trends related to security threats and vulnerabilities.

2.5.9. Reported information security incidents.

2.5.10. Recommendations provided by relevant authorities.

2.5.11. Changes that could affect the organization's approach to manage cyber security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment.

2.6. The output from the management review shall include any decisions and actions related to:

2.6.1. Improvement of the Organization's approach to managing information security and its processes.

2.6.2. Improvement of control objectives and controls.

2.6.3. Improvement in the allocation of resources and or responsibilities.

2.6.4. A documented record of the management review shall be maintained by Enterprise Cyber Security and Governance.

2.6.5. Management approval for the revised policy shall be formally obtained.

COMPLIANCE REFERENCES	**1. ISO 27001:2013 STANDARD** 1.1 Review of the policies for information security (A.5.1) 1.2 Independent review of Information security (A.18.2.1) 1.3 Compliance with security policies and Standards (A.18.2.2) 1.4 Technical compliance review (A.18.2.3) **2. NATIONAL INFORMATION ASSURANCE POLICY (NIA) V2.0** 2.1 Governance Structure [IG] – Section 1.2 (IG 9 – f) **3.** Joint Commission International, Joint Commission International Accreditation Standards for Hospitals. 6th Edition, Joint Commission International: Oak Brook, ILL. 2017 MOI.2 **4. MoPH-** RCFO.9/RCFH.7/ RCP.10
RELATED DOCUMENTS	POL - D - Information Security Management System
REFERENCES	
NAME OF AUTHOR	Mostafa Essemmar, Director – Enterprise Cyber Security and Governance

POLICY OWNER/ DEPARTMENT	Chief Information Officer / Information Technology
APPROVAL BODY	As per Executive Committee Delegation of Authority for Policy Approval (V.4 12 August 2018)
MEASUREMENT OF COMPLIANCE	Security audit and effectiveness measurement
KEYWORD SELECTION	Keyword 1 : Review Keyword 2 : Policy Keyword 3 : Management approval Keyword 4 : Effectiveness

Version Number	Issue Date	Summary of amendments Key Changes	Communication Message
1	21 May 2015	New	
2	13/11/2019	1. Renamed the name of the policy to Cyber Security Management Systems Review. 2. Renamed the information security policy as security policy, IT Security Dept. to Enterprise Cyber Security and Governance Dept. and ISMS (Information Security Management System) to CSMS (Cyber Security Management System) to make it more cyber security specific. 3. Deleted the definition of Information Security Management System. 4. Removed ISO 27001:2013 and NIA from References section.	With the creation of Enterprise Cyber Security and Governance department, it is agreed that Sidra Information Security Management System (ISMS) will be henceforth referred as Sidra Cyber Security Management System (CSMS). The focus will be to maintain the right balance between technical cyber security controls and security governance, risks and compliance related controls in the security policies and procedures. Gradually all the references to the ISMS, Information Security and IT Security department in the security policies and procedures will be replaced with CSMS, Enterprise Cyber Security and Governance, Security Operations respectively.