	Document Title	Document Number	Issue Date
سدرة للطب Sidra Medicine	CYBER SECURITY RISK MANAGEMENT	295	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 Risk Management
PURPOSE	To proactively protect the organization from risks related to Cyber Security that may affect the organization's stated strategic and operational goals and objectives. Provide a consistent risk management framework in which the Cyber Security risks concerning business processes and functions will be identified, considered and addressed in key approval, review and control processes.
APPLICABLE TO	All Sidra staff with access to the organization information or who have been granted access to systems or applications.
DEFINITIONS	
EXPECTED OUTCOME	Align the Cyber Security Risk Management policy with the Enterprise Risk Management policy and embed the Cyber Security Risk Management into the culture and the operations of Sidra, at every level of the organization.

POLICY STATEMENT

1. RESPONSIBILITIES

1.1. Roles and responsibilities of Sidra Board, Audit Risk and Compliance Committee, Chief Executive Team, Enterprise Risk Manager and Executive Director of Governance / Board Secretary shall be as per Section 7 Roles & Responsibilities, of Enterprise Risk Management policy.

1.2. **Sidra Staff**

1.2.1. Sidra staff shall ensure that the way information is handled is in line with the directions given by the organization to safeguard the confidentiality, integrity and availability of the information, and limit the security risks.

1.2.2. Sidra staff shall actively contributes to the identification and mitigation of cyber security risks, and the implementation of the adequate control measures

1.3. **Enterprise Cyber Security & Governance Department**

1.3.1. Ensure the implementation of the cyber security risk management framework and policy.

1.3.2. Monitor the management of significant cyber security risks to ensure that adequate controls are in place to keep risks within acceptable limit.

1.3.3. Identify and evaluate the significant cyber security risks faced by the organization for consideration by senior management.

1.3.4. Apprise Enterprise Risk Manager / Senior management over major decisions taking into consideration the organization's risk profile or exposure.

1.4. **Risk Owner (Business Owner)**

1.4.1. Understand the probability and impact of the existing security risks on the information assets.

1.4.2. Decide on the treatment actions to be taken on identified risks.

1.5. **Action Owner**

1.5.1. Implement the necessary controls to reduce the identified risks as per the approved treatment plan.

1.5.2. Update the Enterprise Cyber Security & Governance and the Risk Owner with the controls implementation plan.

2. METHODOLOGY

2.1. Risk assessment methodology for managing the Cyber Security risks shall be based on the ISO 31000:2018 to meet Risk management requirements of ISO 27001:2013 standard, National Information Assurance Policy v2.0, and Supreme Committee's Cyber Security framework guidelines.

2.2. The security risk assessment shall have a clearly defined scope in order to be effective and should include relationships with risk assessments in other areas.

2.3. The scope of the security risk assessments can be the whole organization, parts of it, an individual information systems, specific system components, or services where this is practicable, realistic and helpful.

2.4. Risks assessments shall identify, quantify, and prioritize security risks against criteria for risk acceptance and objectives relevant to the organization.

2.5. Risk assessment results shall guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

2.6. Risk assessment shall include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

2.7. Risks assessments shall be performed periodically to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur.

2.8. Risk assessments shall be undertaken in a methodical manner capable of producing comparable and reproducible results.

2.9. Identified security risks shall be reported to the Enterprise Risk Manager / senior management as per the Section 5 - Risk Reporting, of POL – O – Enterprise Risk Management policy.

2.10. Criteria for determining whether or not risks can be accepted shall be developed and treatment plans (identified controls to be implemented) shall be developed.

2.11. The effectiveness of the implemented controls shall be periodically assessed and results will be presented to the business owners and used for a new cycle of risk assessment.

COMPLIANCE REFERENCES	**1. ISO 27001:2013 STANDARD** 1.1 Information security risk assessment process (Clause 6.1.2 - ISO/IEC 27001:2013) 1.2 Information security risk treatment (Clause 6.1.3 - ISO/IEC 27001:2013) 1.3 Information security risk assessment Planning (Clause 8.2 - ISO/IEC 27001:2013) 1.4 Information security risk treatment Planning (Clause 8.3 - ISO/IEC 27001:2013) 1.5 Management review (Clause 9.3 - ISO/IEC 27001:2013)

	2. NIA POLICY V2.0 2.1 Risk Management [RM] - Section 2 **3. JCI-** Joint Commission International Accreditation Standards for Hospitals, 6th edition 2017 - MOI.2 **4. MoPH-** RCFO.9/RCFH.7/ RCP.10
RELATED DOCUMENTS	PRO - O - Information Risk Management Methodology POL - O - Enterprise Risk Management
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 : Risk Keyword 2 : Risk management Keyword 3 : Methodology Keyword 4 : Assessment

Version Number	Issue Date	Summary of amendments Key Changes	Communication Message
1	21/05/2017	New	
2	13/11/2019	1. Policy statements are reviewed and rephrased at few places without changing the meaning of the earlier policy statement. 2. Information Risk Management policy is renamed as Cyber Security Risk Management policy and aligned with the POL – O - Enterprise Risk Management policy. 3. Deleted the known definitions Risk Reduction, Risk Acceptance, Risk Avoidance, Risk Transfer as per the DWG guidelines as they can be understood by policy's intended readers. 4. Removed ISO 27001:2013 and NIA from References section to Compliance References.	With the creation of Enterprise Cyber Security & Governance department, it is agreed that Sidra Information Security Management System (ISMS) will be henceforth referred as Sidra Cyber Security Management System (CSMS). Gradually all the references to the Information Risk Management and IT Security in the security policies and procedures will be replaced with Cyber Security Risks and Enterprise Cyber Security and Governance respectively.