	Document Title	Document Number	Issue Date
السدرة Sidra مركز السدرة للطب والبحوث Sidra Medical and Research Center	INFORMATION RISK MANAGEMENT		21 May 2015
		Version Number	First Revision Date
POLICY	APPROVED	#1	20 May 2017
		Version Number	Second Revision Date
		#2	20 May 2019

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

DEPARTMENT	Organizational ☒ Departmental ☐
TITLE	INFORMATION RISK MANAGEMENT
PURPOSE	To proactively protect the organization from risks related to Information Security that may affect the organization's stated strategic and operational goals and objectives. Provide a consistent risk management framework in which the Information Security risks concerning business processes and functions will be identified, considered and addressed in key approval, review and control processes.
APPLICABLE TO	All workforce members with access to the organization information or who have been granted access to systems or applications. All business partners; business associates; full-time, part-time, and temporary employees; contractors; consultants; and vendors.
DEFINITIONS	• **Risk reduction** - or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. • **Risk acceptance** -involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for small risks where the cost of reduction or insuring against the risk would be greater over time than the total losses sustained. • **Risk avoidance** -includes not performing an activity that could carry risk. • **Risk transfer** - sharing with another party the burden of loss or the benefit of gain from a risk and the measures to reduce a risk (insurance measures).
EXPECTED OUTCOME	• Embed Information Security Risk Management into the culture and the operations of Sidra, at every level of the organization • Duties related to information security risk management shall be performed in accordance with the points listed in the policy statements. • Identification, assessment and awareness of existing risks to provide timely information to senior management to drive decisions of risk treatment (risk acceptance, reduction, avoidance or transfer).
POLICY STATEMENT	**1. RESPONSIBILITIES** 1.1. All staff 1.1.1. Ensure that the way information is handled is in line with the directions given by the organization to safeguard information security, integrity and availability, and limit risks.

1.1.2. Contribute actively to the identification and mitigation of Information Security risks, and the implementation of the adequate control measures.

1.2. IT Security Department
- 1.2.1. Ensure the implementation of the information risk management framework and policy.
- 1.2.2. Monitor the management of significant risks to ensure that appropriate controls are in place.
- 1.2.3. Identify and evaluate the significant risks faced by the organization for consideration by senior management.
- 1.2.4. Apprise management over major decisions taking into consideration the organization's information risk profile or exposure.

1.3. Risk Owner (Business Owner)
- 1.3.1. Understand the probability and impact of the existing risks on the information assets.
- 1.3.2. Decide on the treatment actions to be taken on identified risks.

1.4. Control Owner
- 1.4.1. Implement the necessary controls to reduce the identified risks as per the approved treatment plan.
- 1.4.2. Update the IT Security Manager and the Risk Owner with the controls implementation plan.

2. METHODOLOGY

2.1. Risk assessment methodology for managing the Information Security risks shall be based on the ISO 31000:2009 to meet Risk management requirements of ISO 27001:2013 standard and National Information Assurance Policy v2.0

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

2.10. 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-** MOI.2 4. **MoPH-** RCFO.9/RCFH.7/ RCP.10
RELATED DOCUMENTS	PRO – O - Information Risk Management Methodology
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. 3. Joint Commission International, Joint Commission International Accreditation Standards for Hospitals. 6th Edition, Joint Commission International: Oak Brook, ILL. 2017
NAME OF AUTHOR	Mostafa Essemmar, Manager - IT Security, Infrastructure & Operations Dept
POLICY OWNER/ DEPARTMENT	Chief Information Officer / Information Technology
MEASUREMENT OF COMPLIANCE	Security audit and effectiveness measurement
KEYWORD SELECTION	Keyword 1 : Risk Keyword 2 : Risk management Keyword 3 : Methodology Keyword 4 : Assessment