	Document Title	Document Number	Issue Date
	INFORMATION SECURITY MANAGEMENT REVIEW		**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 SECURITY MANAGEMENT REVIEW
PURPOSE	To ensure that the information security policies, procedures and other key components of the information security management system (ISMS) framework are reviewed at planned intervals, or if significant changes occur to ensure the suitability, adequacy, and effectiveness.
APPLICABLE TO	All workforce members with access to the organization's 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	• **ISMS - Information Security Management System:** that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
EXPECTED OUTCOME	A documented periodic review of information security policies, procedure and the effectiveness measurement of the ISMS.
POLICY STATEMENT	**1. REVIEW CYCLE** 1.1. The information security policies shall be reviewed annually 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 at any time, with or without prior notice to the operational community. 1.3. As soon as practical after a policy revision and approval provided by the authorized level of management, the IT Security Department will provide notification to the operational community that the policy has been revised. **2. REVIEW ENFORCEMENT** 2.1. The organization's approach to managing information security and its implementation

	(i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur. 2.2. Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. 2.3. Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards. 2.4. All information security policies shall have a designated owner, who has approved management responsibility for the development, review, and evaluation of the security policies. 2.5. The review of the information security policy shall take into account the results of management reviews. 2.6. Inputs for the review shall include information on: 2.6.1. Feedback from interested parties. 2.6.2. Results of independent reviews, which may be internal or external audits. 2.6.3. Status of preventive and corrective actions. 2.6.4. Process performance and information security compliance. 2.6.5. Results of previous management reviews. 2.6.6. Trends related to threats and vulnerabilities. 2.6.7. Reported information security incidents. 2.6.8. Recommendations provided by relevant authorities. 2.6.9. Changes that could affect the organization's approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment. 2.7. The output from the management review shall include any decisions and actions related to: 2.7.1. Improvement of the Organization's approach to managing information security and its processes. 2.7.2. Improvement of control objectives and controls. 2.7.3. Improvement in the allocation of resources and or responsibilities. 2.7.4. A documented record of the management review shall be maintained. 2.7.5. 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 v2.0** 2.1 Governance Structure [IG] – Section 1.2 (IG 9 – f) **3. JCI-** MOI.2 4. **MoPH-** RCFO.9/RCFH.7/ RCP.10
RELATED DOCUMENTS	POL – D - Information Security Management System
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 : Review Keyword 2 : Policy Keyword 3 : Management approval Keyword 4 : Effectiveness