سدرة للطب Sidra Medicine	Document Title	Document Number	Issue Date
	Third Party Security Management		24/04/2016
		Version Number	Revision Date
POLICY	APPROVED	#1	30/06/2018

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 ☒ Name: Information Management
TITLE	Third Party Security Management
PURPOSE	Maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
APPLICABLE TO	Full-time or part-time Third Party vendors, suppliers, service providers or consultants that are contracted for a definite period of time.
DEFINITIONS	**Third Party -** Individual or organization having a contractual or regulatory relationship and that is not a member of the organization (Employees or Board of Directors).
EXPECTED OUTCOME	Implement and maintain the appropriate level of information security and service delivery in line with Third Party service delivery agreements.
POLICY STATEMENT	**1. GENERAL** 1.1 All Third Party personnel/ organizations having access to Sidra's classified information and information processing facilities shall adhere to relevant the security policies. 1.2 Any physical and logical access given to Third Party personnel shall be pre-approved, logged and monitored. **2. SECURITY IN THIRD PARTY AGREEMENTS** 2.1 All Third Party entities shall sign a confidentiality and non-disclosure agreement before being provided access to internal or confidential information. 2.2 Information security and the protection of confidential information shall be addressed in all Third Party contract agreements. 2.3 Information technology outsourcing agreement shall include clauses concerning service provider's regular testing and maintenance of system security on an on-going basis. 2.4 Agreements shall include a "Right to Audit" clause ensuring the organization's personnel and/or an authorized representative could physically and logically evaluate a Third Party's control environment. 2.5 Ownership of software developed by outsourced personnel (e.g., contractors) shall be defined in the contract agreement. 2.6 The organization's group responsible for the selection and approval of Third Party services and a representative from Legal Department shall approve all contracted information services agreements. Approval from IT/ Information Security shall also be obtained if the

	services provided affect the security or integrity of the organization's networks or confidential information. 2.7 All security roles and responsibilities shall be defined and communicated to the Third Party contractor. **3. MONITORING AND REVIEW OF THIRD PARTY SERVICES** 3.1 Compliance and adherence of third parties to security controls and agreement shall be monitored and assessed through the IT/Information security annual risk assessment. 3.2 Depending on the sensitivity and criticality of the services or data provided, an independent audit report shall be provided or an IT/ Information Security audit exercise shall be performed. 3.3 Changes to the Third Party services that would impact the provided access to information, systems and business processes shall be assessed and security clauses in agreements updated if necessary.
COMPLIANCE REFERENCES	**1. ISO 27001:2013 Standard** 1.1 Information security policy for supplier relationships (A.15.1.1) 1.2 Addressing security within supplier agreements (A.15.1.2) 1.3 Information and communication technology supply chain (A.15.1.3) 1.4 Monitoring and reviewing of supplier services (A.15.2.1) 1.5 Managing changes to supplier services (A.15.2.2) **2. NIA Policy v2.0** 2.1 Governance Structure [IG] – Section 1.2 2.2 Third Party Security Management [TM] – Section 3.2 2.3 Appendix D (Informative) – sample Non-Disclosure Agreement (NDA) 3. **JCI**- MOI.2 4. **MoPH-** RCFO.9/RCFH.7 / RCP.10
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. **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 Services
MEASUREMENT OF COMPLIANCE	Periodic Security Audits
KEYWORD SELECTION	Keyword 1 : Third Party Keyword 2 : Supplier Keyword 3 : Non-disclosure Keyword 4 : Agreement