	Document Title	Document Number	Issue Date
سدرة للطب Sidra Medicine	**THIRD PARTY SECURITY MANAGEMENT**	**544**	**08/10/2019**
	Approved By	**Version Number**	**Review Due Date**
POLICY	**Joanna Smith – Chief Information Officer**	**2**	**08/10/2021**

SCOPE	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	
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 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 (NDA) 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 authorized personnel and/or representative from Sidra could physically and logically evaluate a Third Party's environment.

2.5 Ownership of software developed by outsourced personnel (e.g., contractors) shall be clearly 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 should be 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. National Information Assurance (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	
NAME OF AUTHOR	Naoufal Rihani, Head of Information Security
POLICY OWNER/ DEPARTMENT	Director – Enterprise Cyber Security & Governance
APPROVAL BODY	As per Executive Committee Delegation of Authority for Policy Approval (V.4 12 August 2018)
MEASUREMENT OF COMPLIANCE	Periodic Security Audits
KEYWORD SELECTION	Keyword 1 : Third Party Keyword 2 : Supplier Keyword 3 : Non-disclosure Keyword 4 : Agreement

Version Number	Issue Date	Summary of amendments Key Changes	Communication Message
1	24/04/2016	New	
2	08/10/2019	1- No major amendments have been made to the policy. The Policy statements are still relevant as per the industry best Third Party Security monitoring practices. Minor changes have been made to the policy statements (rephrased the policy statement) without changing its meaning. 2- Deleted the definition of Third Party as it's easily understood by the intended readers. (As per the DWG guidelines) 3- Moved ISO 27001:2013, NIA and JCI from References section to Compliance References.	