	Document Title	Document Number	Issue Date
سدرة للطب Sidra Medicine	IT Security Incident 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	IT Security Incident Management
PURPOSE	Ensure an efficient framework for reporting and management of security incidents is in place, to promote a reduction in the number of security incidents, and help prevent new incidents from occurring.
APPLICABLE TO	Information processing systems, information processing facilities, information assets, and applications used by the Sidra staff, vendors and third party contractors.
DEFINITIONS	**Information Security Incident -** An Information Security Incident is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations. The incident categories used for classification are: ▪ Non-Conformity - To information security policies ▪ Asset Theft / Loss - Intentional/ unintentional stealing, misplacing or disclosure of Sidra non-public information ▪ Abuse – Unauthorized use of resources or system for non-business related purpose. ▪ Access - Unauthorized Access to a service or a system through the bypass of security controls. ▪ Viruses and Security Vulnerabilities – Virus attacks, intrusion attempts, and detection of security vulnerabilities in systems and business processes.
EXPECTED OUTCOME	Implement an incident management process in accordance with the rules set out in the policy statement to minimize adverse impacts and gather appropriate forensic evidence.
POLICY STATEMENT	**1. INCIDENT REPORTING** 1.1 All IT security incidents and security-related events that could have an adverse impact on the organization's operations or the privacy and protection of sensitive hospital, research, or educational information must be immediately reported to the business or clinical manager, the IT Service Desk, or the IT Security Manager. This applies to all workforce members, including contractors, consultants, and 3rd party users. 1.2 All employees and contractors shall be made aware of their responsibility to report information security events in a timely manner. 1.3 Wherever feasible, IT Security shall employ automated mechanisms to assist in the reporting of security incidents. **2. REPORTING INFORMATION SECURITY WEAKNESSES**

2.1 Employees and contractors using the organization's information systems and services shall report any observed or suspected information security weaknesses in systems or services.
2.2 Employees and contractors shall not perform any type of technical assessments using scanning and systems penetration techniques.

3. MANAGEMENT OF INFORMATION SECURITY INCIDENTS

3.1 A consistent and effective approach shall be applied to the management of Information Security Incidents.
3.2 Specific criteria shall be developed for incident categorization based on the impact severity on assets, end users and business processes.

4. INCIDENT HANDLING

4.1 The IT Service Desk, in coordination with IT Security, shall implement an incident handling capability for security incidents and events reporting and management.
4.2 Incident handling shall include detection, reporting, analysis, containment, and recovery processes.
4.3 Wherever feasible, automated mechanisms to support the incident handling process shall be implemented.

5. COLLECTION OF EVIDENCE

5.1 Where follow-up action after an Information Security Incident involves legal action (either civil or criminal):
5.1.1 Evidence shall be collected, retained, and presented in a non-modified form.
5.1.2 Only trained and certified computer forensic and security specialists shall engage in the retrieval and collection of forensic evidence for any civil action or criminal prosecution.
5.1.3 The proper chain of custody shall be maintained for any evidence collected during the investigation of a security incident.

6. LEARNING FROM INFORMATION SECURITY INCIDENTS

6.1 Knowledge gained from analyzing and resolving Information Security Incidents shall be used to reduce the likelihood or impact of future incidents.
6.2 There shall be mechanisms in place to enable the types, volumes and impact of Information Security Incidents to be quantified and monitored.
6.3 The information gained from the evaluation of Information Security Incidents shall be used to identify recurring or high impact incidents

7. DOCUMENTATION AND REPORTING TO MANAGEMENT

7.1 Security incidents shall be documented and tracked.
7.2 The systems administrators shall provide the information and documentation required to perform the investigation and complete the reporting of any security incident involving their respective systems.
7.3 IT Security shall maintain an incident log register and regularly report high severity incidents and overall incident trend to the management.

8. INCIDENT RESPONSE TRAINING

8.1 Employees and contractors shall be made aware of the procedures for reporting the different types of security events and incidents that might have an impact on Sidra assets.
8.2 An awareness program covering incident detection, reporting and handling shall be developed and implemented.

COMPLIANCE REFERENCES

1. ISO 27001:2013 Standard

1.1 Responsibilities and procedures (A.16.1.1)
1.2 Reporting information security events (A.16.1.2)
1.3 Reporting information security weaknesses (A.16.1.3)
1.4 Assessment of and decision on information security events (A.16.1.4)
1.5 Response to Information Security Incidents (A.16.1.5)
1.6 Learning from Information Security Incidents (A.16.1.6)

2. NIA Policy v2.0

2.1 Access Control Security [AM] – Section 9.2
2.2 Governance Structure [IG] – Section 1.2

	2.3 Portable Devices & Working Off-Site Security [OS] – Section 11.2 2.4 Physical Security [PH] – Section 11.2 2.5 APPENDIX C – Incident Management Criticality Classification 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- IT Security, Infrastructure & Operations Dept
POLICY OWNER/ DEPARTMENT	Chief Information Officer / Information Technology Services
MEASUREMENT OF COMPLIANCE	Periodic Security Audits Annual Effectiveness Review
KEYWORD SELECTION	Keyword 1 : Incident Keyword 2 : Evidence Keyword 3 : Response Keyword 4 : Investigation