سدرة للطب Sidra Medicine	Document Title	Document Number	Issue Date
	CYBER SECURITY INCIDENT MANAGEMENT	**538**	**10/11/2019**
	Approved By	**Version Number**	**Review Due Date**
POLICY	**Chief Information Officer**	**2**	**10/11/2021**

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

SCOPE	Organizational ☒ Departmental ☐
TITLE	Cyber 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	Sidra staff having access to information processing systems, information processing facilities, information assets, and applications.
DEFINITIONS	
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, (e.g.: non-conformity to IT Security policies, virus, security vulnerabilities, successful phishing or ransomware attacks) that could have an adverse impact on the daily operations and information of Sidra must be immediately reported to the IT Security department. . This applies to all Sidra staff including 3rd party contractors and consultants.

1.2 Sidra staff and contractors shall be made aware of their responsibility to report security events in a timely manner.

1.3 Wherever feasible, IT Security shall deploy automated mechanisms to assist in the reporting of security incidents.

2. REPORTING INFORMATION SECURITY WEAKNESSES

2.1 All Sidra staff and contractors using the organization’s information systems and services shall report any observed or suspected security weaknesses in systems or services.

2.2 Only Sidra authorized staff and contractors shall 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 IT Security Incidents.

3.2 Specific criteria shall be developed for incident categorization based on the severity of impact on assets, end users and business processes.

4. INCIDENT HANDLING

4.1 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.

5.1.4 The General Counsel shall be notified of such action.

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. National Information Assurance (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	PRO - O - Security Incident Management
REFERENCES	
NAME OF AUTHOR	Mostafa Essemmar- Director – Enterprise Cyber Security & Governance

POLICY OWNER/ DEPARTMENT	Chief Information Officer / Information Technology Services	
MEASUREMENT OF COMPLIANCE	Periodic Security Audits Annual Effectiveness Review	
KEYWORD SELECTION	Keyword 1 : Incident Keyword 3 : Response	Keyword 2 : Evidence Keyword 4 : Investigation

Version Number	**Issue Date**	**Summary of amendments Key Changes**	**Communication Message**
1	21/04/2016	New procedure	
2	10/11/2019	Reviewed. Renewal with minor amendment endorsed by document Owner. Minor amendment(s) as follows: • No major amendments have been made to the document. References to IT Service Desk in policy statement 1.1 and 4.1 have been removed as IT Security has now setup a full-fledged security incident handling capability for quick resolution. • Deleted the definition of Information Security Incident, as they are clearly understood to the intended readers of the procedure. (As per the DWG guidelines) • Moved ISO 27001:2013 and NIA from References section to Compliance References. • Due to the nature of IT security incidents, proposing to covert this departmental policy to organizational policy**.**	Departmental policy will be communicated throughout the department respective staff.