	Document Title	Document Number	Issue Date
سدرة للطب Sidra Medicine	**SYSTEM SECURITY MONITORING**	**543**	**10/10/2019**
	Approved by	**Version Number**	**Review Due Date**
POLICY	**Joanna Smith – Chief Information Officer**	**2**	**10/10/2021**

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	System Security Monitoring
PURPOSE	Set the controls required for monitoring information systems.
APPLICABLE TO	System events and alerts generated by the Information processing systems, applications, database and servers that are logged and monitored by the authorized Sidra IT staff, vendors and third party contractors.
DEFINITIONS	
EXPECTED OUTCOME	Systems shall be monitored and information security events shall be recorded as per the policy statements.

POLICY STATEMENT

1. MONITORING SYSTEM USE

1.1 Monitoring of systems and incident response mechanism shall be implemented on a continuous 24x7 basis.

1.2 Critical Security Logs and alerts shall be reviewed and analyzed at least daily and follow-up to exceptions performed when required.

1.3 The level of monitoring required for individual facilities shall be determined by a risk assessment. Areas that shall be considered include:

- 1.3.1 Authorized access, including detail such as:
  - 1.3.1.1 User ID
  - 1.3.1.2 Date and time of key events
  - 1.3.1.3 Types of events
  - 1.3.1.4 Files accessed
  - 1.3.1.5 Program or utilities used
- 1.3.2 All privileged operations, such as:
  - 1.3.2.1 Use of privileged accounts
  - 1.3.2.2 System start-up and stop
  - 1.3.2.3 Input/output device attachment or detachment
- 1.3.3 Unauthorized access attempts, such as:
  - 1.3.3.1 Failed or rejected user actions
  - 1.3.3.2 Failed or rejected actions involving data and other resources
  - 1.3.3.3 Access policy violations and notifications for network gateways and firewalls
  - 1.3.3.4 Alerts from proprietary intrusion detection/prevention systems
- 1.3.4 System alerts or failures such as:
  - 1.3.4.1 Console alerts or messages
  - 1.3.4.2 System log exceptions
  - 1.3.4.3 Network management alerts
  - 1.3.4.4 Alarms raised by the access control system
  - 1.3.4.5 Changes to, or attempts to change, system security settings and controls

2. ADMINISTRATOR AND OPERATOR LOGS

2.1 System administrator and system operator activities shall be logged.

2.2 The logs shall include:

2.2.1 Time at which an event occurred

2.2.2 Information about the event or failure

2.2.3 Which account and which administrator was involved

2.2.4 Which purposes was involved

3. FAULT LOGGING

3.1 Faults shall be logged, analyzed, and appropriate actions shall be taken for rectification of error.

3.2 A record of faults reported by users or identified by system programs on critical information processing and communications systems shall be maintained.

3.3 Incident response procedures shall be followed while reporting suspicious fault logging attempts.

4. CLOCK SYNCHRONIZATION

4.1 The clocks of all relevant systems shall be synchronized with an agreed time source.

4.2 System administrators shall ensure synchronization of their respective systems with the agreed time source to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

5. PROTECTION OF LOG INFORMATION

5.1 Audit logs shall be retained for at least one (1) year with a minimum of three (3) months immediately available for analysis (online, archived, or restorable from back-up).

5.2 Wherever feasible, there shall be segregation of duties between system use and System Monitoring.

5.3 Logging facilities and log information shall be protected against tampering and unauthorized access. This includes:

5.3.1 Alterations to the message types that are recorded

5.3.2 Log files being edited or deleted

5.3.3 Storage capacity to be monitored to prevent failure to record events or over writing of past recorded events

COMPLIANCE REFERENCES	**1. ISO 27001:2013 Standard** 1.1 Event logging (A.12.4.1) 1.2 Protection of log information (A.12.4.2) 1.3 Administrator and operator logs (A.12.4.3) 1.4 Clock Synchronization (A.12.4.4) 1.5 Management of technical vulnerabilities (A.12.6.1) 1.6 Information system audit controls (A.12.7.1 **2. National Information Assurance (NIA) Policy v2.0** 2.1 Logging & Security Monitoring [SM] – Section 10 **3. Joint Commission International, Joint Commission International Accreditation Standards for Hospitals. 6th Edition, Joint Commission International: Oak Brook, ILL. 2017** **JCI-** MOI.2 **MoPH-** RCFO.9/RCFH.7/ RCP.10
RELATED DOCUMENTS	PRO – D – Security Incident Management
REFERENCES	
NAME OF AUTHOR	Naoufal Rihani, Head of Information Security
POLICY OWNER / DEPARTMENT	Mostafa Essemmar, 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 Annual Effectiveness Review
KEYWORD SELECTION	Keyword 1 : Log Keyword 2 : Audit Log Keyword 3 : Monitoring Keyword 4 : Clock Synchronization

Version Number	Issue Date	Summary of amendments Key Changes	Communication Message
1	21/04/2016	New	
2	10/10/2019	1- No major amendments have been made to the policy. The Policy statements are still relevant as per the industry best systems security monitoring practices. 2- Deleted the definitions of Security Monitoring and Security Log as they are specific to the departmental policy and will be easily understood by its intended readers. (As per the DWG guidelines) 3- Moved ISO 27001:2013, NIA and JCI from References section to Compliance References.	