<table>
<thead>
<tr>
<th>DEPARTMENT</th>
<th>Organizational</th>
<th>Departmental</th>
<th>Name: Information Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>TITLE</td>
<td>System Security Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PURPOSE</td>
<td>Set the controls required for monitoring information systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APPLICABLE TO</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| DEFINITIONS      | **System Monitoring** - Process within a distributed system for collecting and storing data  
**Security Log** - Contains records of login/logout activity or other security-related events specified by the system's audit policy. The Security Log is one of the primary tools used by Administrators to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems. |
| 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:
      - User ID
      - Date and time of key events
      - Types of events
      - Files accessed
      - Program or utilities used
      1.3.2 All privileged operations, such as:
      - Use of privileged accounts
      - System start-up and stop
      - Input/output device attachment or detachment
      1.3.3 Unauthorized access attempts, such as:
      - Failed or rejected user actions
      - Failed or rejected actions involving data and other resources
      - Access policy violations and notifications for network gateways and firewalls
      - Alerts from proprietary intrusion detection/prevention systems
      1.3.4 System alerts or failures such as:
      - Console alerts or messages
      - System log exceptions
      - Network management alerts
      - Alarms raised by the access control system
      - 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:
       - Time at which an event occurred
       - Information about the event or failure
       - Which account and which administrator was involved
       - Which purposes was involved

3. FAULT LOGGING
   3.1 Faults shall be logged, analyzed, and appropriate actions 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:
       - Alterations to the message types that are recorded
       - Log files being edited or deleted
       - 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. NIA Policy v2.0  
| | 2.1 Logging & Security Monitoring [SM] – Section 10  
| | 3. JCI- MOI.2  
| | 4. MoPH- RCFO.9/RCFH.7/ RCP.10  

| RELATED DOCUMENTS | POL - D - Media Retention and Disposal  


| 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 : Log  
| | Keyword 2 : Audit Log  
| | Keyword 3 : Monitoring  
| | Keyword 4 : Clock Synchronization  

Sidra Policy Template v1.0