| سدرة للطب<br>Sidra Medicine | Document Title | Document Number | Issue Date |
|---|---|---|---|
| | **NETWORK SECURITY** | **541** | **27/10/2019** |
| | **Approved By** | **Version Number** | **Review Due Date** |
| **POLICY** | **Chief Information Officer** | **2** | **27/10/2021** |

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** | Network Security |
| **PURPOSE** | Specify the security rules related to the organization’s networks infrastructure. |
| **APPLICABLE TO** | Network and security appliances, information processing systems, applications and servers accessed and managed by the authorized Sidra IT staff, vendors and third party contractors. |
| **DEFINITIONS** | |
| **EXPECTED OUTCOME** | Networks Security controls implemented and organization’s network managed and as per the rules set out in the policy statement. |

## POLICY STATEMENT

### 1. GENERAL STATEMENTS

1.1 Defense in depth strategy that layers security mechanisms shall be implemented.
1.2 Logical access to the organization’s network and network activity must be restricted.
1.3 The network shall use demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between any external entities and the internal network.
1.4 Network topology shall have multiple layers, with the most critical communications occurring in the most secure and reliable layer.
1.5 Physical access to the organization’s network and devices shall be restricted.
1.6 A combination of physical access controls shall be used to secure data centers, telecommunications rooms, and other physical locations where critical infrastructure assets are located.
1.7 Security patches shall be deployed promptly after testing under field conditions.
1.8 All unused ports and services must be disabled.
1.9 User privileges must be restricted to those that are required for each workforce member’s role.
1.10 Audit trails must be tracked and monitored.
1.11 Security controls such as anti-virus software and file integrity-checking software must be employed whenever applicable.
1.12 Each critical component of the network infrastructure shall have a redundancy built in for high availability.
1.13 Groups of information services, users, and information systems shall be segregated on networks.
1.14 A purpose based Network Clock shall be implemented and all organization’s systems shall be synchronized to it as a single reference time source.

## 2. NETWORK SECURITY ACCESS CONTROLS

2.1 Access control mechanisms, auditing mechanisms, intrusion detection/prevention systems, and disaster recovery plans, shall be used to protect the organization networks.

2.2 Network devices shall be configured and safeguarded against unauthorized access and must be routinely audited and monitored.

## 3. NETWORK ADMINISTRATION

3.1 Only fully qualified and authorized IT network and security personnel shall be granted access to network and security devices.

3.2 Network managers and administrators must be knowledgeable of the threats and vulnerabilities to the devices they manage and the risks inherent in each.

3.3 Network managers and administrators must be fully trained and have sufficient experience in the network devices for which they are assigned responsibilities.

## 4. NETWORK INTRUSION DETECTION/PREVENTION SYSTEM

4.1 Network/host-based intrusion detection systems (IDS) and/or network/host-based intrusion prevention systems (IPS) shall be implemented and configured to;

4.1.1 Monitor and analyze inbound and outbound communications for unusual or unauthorized traffic.

4.1.2 Employ automated tools to support near-real-time analysis of events, which enable timely detection and response to security incidents.

## 5. NETWORK FIREWALLS

5.1 All connections between the organization’s network and public networks shall pass through a security firewall where access can be examined, evaluated, and either permitted or rejected according to pre-defined rules.

5.2 To provide consistent configuration of all organization’s firewall services, firewall administrators must comply with the following minimum guidelines:

5.2.1 Firewall security policy requires “deny by default” for all firewall configurations.

5.2.2 All open ports and services must have a documented business justification.

5.2.3 All ports and services shall be filtered or restricted to specific systems that need them. This includes both inbound and outbound traffic.

5.3 Blocking access to specific services may adversely affect connectivity, productivity or functionality. When a service is needed, the access at the firewall must be:

5.3.1 Restricted to those specific systems that require the service;

5.3.2 Monitored, either through the firewall logging functionality or by having an intrusion detection system in place to monitor the restricted side of the firewall;

5.3.3 Fully documented, with a justification from the business operation requesting the service;

5.4 Firewall rule base review shall be performed on a regular basis. All firewall rules shall be justified and approved by IT Security and timely corrections implemented when required.

## 6. Network Configuration Diagram

6.1 Network Configuration diagram shall be kept confidential and made available only on need to know basis after the approval of IT Security.

6.2 Network configuration diagram shall be updated as and when changes are done, latest network diagram shall be aligned with Disaster Recovery Plan.

| | |
|---|---|
| **COMPLIANCE REFERENCES** | 1. ISO 27001:2013 Standard<br>1.1 Network Controls (A.13.1.1)<br>1.2 Security of network services (A.13.1.2)<br>1.3 Segregation in networks (A.13.1.3)<br>1.4 Information transfer policies and procedures<br>1.5 Administrator and Operator Logs (A.12.4.3)<br>1.6 Event Logging (A.12.4.1)<br>1.7 Clock Synchronization (A.12.4.4)<br>1.8 Limitation of connection time (A.11.5.6)<br>1.9 Access control policy (A.9.1.1)<br>1.10 Installation of soft- ware on operational systems (A.12.5.1)<br>1.11 Securing application services on public networks (A.14.1.2)<br>1.12 Protecting application services transactions (A.14.13)<br>2.1 National Information Assurance (NIA) Policy v2.0. Network Security [NS] – Section 2 |

| | |
|---|---|
| | 3 Joint Commission International, Joint Commission International Accreditation Standards for Hospitals. 6th Edition, Joint Commission International: Oak Brook, ILL. 2017 – JCI MOI.2<br>4 MoPH- RCFO.9/RCFH.7/ RCP.10 |
| **RELATED DOCUMENTS** | |
| **REFERENCES** | |
| **NAME OF AUTHOR** | Mostafa Essemmar, Director - Enterprise Cyber Security and Governance |
| **POLICY OWNER/ DEPARTMENT** | Executive Director - Infrastructure and Operations / Information Technology Services |
| **APPROVAL BODY** | As per Executive Committee Delegation of Authority for Policy Approval (V.4 12 August 2018) |
| **MEASUREMENT OF COMPLIANCE** | Periodic Security Audits<br>Annual Effectiveness Review |
| **KEYWORD SELECTION** | Keyword 1 : Network Keyword 2 : Firewall<br>Keyword 3 : Intrusion Prevention |

| Version Number | Issue Date | Summary of amendments Key Changes | Communication Message |
|---|---|---|---|
| 1 | 21/04/2016 | New | |
| 2 | 27/10/2019 | Reviewed. Renewal with minor amendment endorsed by document Owner.<br>Minor amendment(s) as follows:<br>• No amendments / changes have been made to the policy. All Policy statements are still relevant as per the industry best Network Security practices.<br>• Moved ISO 27001, NIA and JCI references to Compliance Reference section. | Departmental Policies are published in the portal and are communicated to respective staff through departmental means. |