

Network Security

SardineAI Corp. (SardineAI)

May 22, 2026

Table of Contents

Network Security 3

Sardine Network Security Policy 3

1.0 Purpose 3

2.0 Scope 3

3.0 Policy 3

3.1 Network Security Management 3

3.2 Third Party Interconnection 4

3.3 Logging and Monitoring 4

3.4 Set Correct Time and Date 5

3.5 Backup Network Device Configuration 5

3.6 Router Security 5

3.7 Switch Security 5

3.8 Network Design and Audits 5

3.9 Encrypt Sensitive Network Traffic 6

3.10 Develop and Maintain Expertise 6

3.11 Patching 6

6.0 Enforcement 6

7.0 Document Control 7

Network Security

Sardine provides a protected, interconnected computing environment through the use of securely configured network devices to meet organizational missions, goals, and initiatives.

Sardine Network Security Policy

1.0 Purpose

One of Sardine's objectives is to secure its internal network, network connections and resources from intrusions and to provide/maintain the security of Sardine infrastructure and data and thus this policy provides guidelines to ensure availability and reliability of network devices for safe and secure connections to the information assets owned by Sardine.

2.0 Scope

This policy applies to all network devices (routers, switches, wireless access points, firewalls, other network services) that are owned and managed by Sardine or its affiliate(s). This policy shall be applicable to the entire IT Network administration related work including design, installation, testing, support and management

3.0 Policy

Sardine's network and public web sites shall be secured against intrusions and network failures that would affect confidentiality, availability and integrity of information and information assets.

Interconnection of networks between SardineAI and third parties (vendors, customers and subsidiaries) shall be provided after a formal risk assessment and authorization.

Sardine networks shall be segregated from external networks by firewalls. SardineAI shall maintain due care for protecting the customer network interconnecting to its own from threats originating from within SardineAI.

3.1 Network Security Management

Network devices owned and managed by SardineAI must be configured securely and designed to secure network traffic between trusted and untrusted network zones.

Every network device deployed in the SardineAI network shall be appropriately configured and meet security requirements for their individual purposes (internal, public facing, demilitarized zones (DMZ)).

All traffic and protocols should be expressly denied except for those necessary for business purposes.

The SardineAI network shall be isolated from unsecured networks, Internet and third party networks through firewalls and intrusion detection systems. The IT department shall assess if personal firewalls should be installed on workstations.

All remote access to SardineAI systems shall be through an authorized medium like VPN is made available with appropriate risk assessment and based on authorizations.

All intranet users originating connections from the Internet shall be authenticated, over an encrypted connection. The password policy is strictly enforced for all applications used over the Internet.

Job responsibilities will be segregated for personnel assigned for Network operations and computer operations whenever practical.

The information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

3.2 Third Party Interconnection

There shall be a third party agreement with vendors, customers or partners before interconnecting with the SardineAI network.

Customer or partner networks interconnecting with the SardineAI network would be isolated from each other.

All customer traffic over a dedicated link would be encrypted using appropriate technology and VPN connections if required by the customer.

Access to customer networks shall be granted only to specific SardineAI employees based on business need and after proper authorization.

3.3 Logging and Monitoring

Logging should be enabled, including log configuration changes, preferably back to a central source like a syslog server or a centralized log management platform.

All administrator access to the network and network security products should be authorized, logged and monitored. All network services and their use shall be monitored by SardineAI's IT team. All firewall traffic should be monitored for possible misuse and intrusions.

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

3.4 Set Correct Time and Date

Synchronize network device clocks with Network Time Protocol (NTP). The appropriate time zone should be set for all equipment.

3.5 Backup Network Device Configuration

Network device configuration is backed up regularly or whenever configuration changes are made to a central source. The central backup source shall be secured as well.

3.6 Router Security

Physical Security (when applicable)

Routers and switches must be located in a locked room and not accessible to unauthorized personnel. Devices must have adequate cooling, a reliable power supply and/or plugged into a right-sized uninterruptible power supply (UPS). Wireless access points should either be in a locked room or located high on the ceiling where it would be obvious if someone were physically accessing the device.

Privilege Access Control

- Routers must be secured with complex passwords for all interfaces including the Console, AUX, and VTY (telnet/ssh) interfaces (to prevent initial access).
- Privileged access to prevent configuration changes should be restricted to authorized personnel only.
- Passwords shall follow strong password mechanisms outlined under the Password Guidelines.
- Access control shall be used to provide separate authentication, authorization, and accounting services for network-based access.
- A Privileged Access Management solution can control credentials accessing the device and commands that can be executed when a session is initiated, providing a complete audit of both commands and sessions.

3.7 Switch Security

Switch ports shall be locked down by configuring port security features allowing access only to the first authorized device connecting to that port.

3.8 Network Design and Audits

- Network design shall allow legitimate traffic to flow through the appropriate zones, segments and/or resources, and unwanted traffic detected and dropped. Firewalls, Virtual Local Area Networks (VLANs) and/or Access Control Lists (ACLs) shall be implemented to achieve the same.
- Development/testing, production and corporate resources should not be in the same network segments.
- IP phones and IoT devices should be logically separated on the network.
- The network diagram should provide an overview of network devices deployed, network traffic flows and should identify physical and/or logical security controls that are in place to direct legitimate traffic and detect & drop unnecessary or unwanted traffic.
- Firewall policies and ACLs shall be tested to ensure that whatever is not permitted is denied. The network shall be audited based on the network diagram by conducting vulnerability scans and penetration tests on strategic areas in the network and mitigate identified high risks.

3.9 Encrypt Sensitive Network Traffic

Appropriate encryption and authentication methods should be used for the transmission of sensitive data and remote access.

3.10 Develop and Maintain Expertise

Ensure that network support personnel are adequately trained in implementing and supporting a secured network infrastructure through training and drills.

3.11 Patching

Network devices shall be patched and updated on a documented, regular, and timely schedule. Common Vulnerability Scoring System (CVSS) is recommended to be used to aid in setting patching guidelines.

Applicable critical vendor-supplied security patches shall be applied within a defined time frame after release and installation of all other applicable vendor-supplied security patches as per the defined patching schedule.

In addition to the patching guidelines, vulnerabilities and exploitable findings deemed critical by the SardineAI, regardless of CVSS score, must be patched as soon as possible.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Document Control

Version	Date	Updated By	Approved By	Notes
2.2	2025-05-22	Blaine Northcraft	Bil Corry	Annual review
2.1	2024-05-20	Blaine Northcraft	Bil Corry	Annual review, added enforcement and document control sections
2.0	5/23/2023	Blaine Northcraft	Bil Corry	Updated Scope
1.0	1/29/2021	Zahid Shaikh	Zahid Shaikh	Initial Draft