NETWORK MANAGEMENT POLICY

CHANGE HISTORY

Date	Version	Created by	Approved By	Description of change
08/10/2024	1.0	Bharath S	Ashwin Khosla	Basic document outline and submitted for review

Purpose

Purpose of this policy is to establish standards for protecting networks and firewalls in Veranda Learning.

Scope

This policy applies to all networks

- Internal networks managed by Veranda Learning
- Cloud hosted networks managed by Veranda Learning
- Other third-party networks

Background

Networks are an essential component of all companies' security infrastructure, which manages connectivity and data flow to and from its information systems. As a result, it is critical to protect the networks from unauthorized access, malicious code, unwanted traffic, etc. Failure to protect the network will very easily lead to attacks such as

- Denial of service
- Ransomware
- Data breaches, loss, and theft
- Introduction of malicious code

Policy

Documenting the network

All network patterns and high-level data flow at Veranda Learning are documented and regularly reviewed and updated as required. The documentation, at the minimum, includes

- A diagram of permissible paths with a justification for each,
- A description of permissible services, ports, and protocols
- VPCs, Private and Public Subnets
- VPNs, Firewalls

All ports, protocols, and connectivity will default to DENY

Every connectivity path and service is blocked. The connectivity can be opened only by specific requests made or needed.

Internal connections between machines

Real-time connections between user machines and production machines must be disabled by default and be enabled only by special requests using bastion servers, security groups, white labeling, firewalls, or other access control methods.

Secured Subnets & demilitarized zone (DMZ)

Secure servers such as databases should be disconnected from the public network and be deployed on their own private subnet. Access to this and other subnets should be restricted with firewalls and other access control measures.

Encryption of traffic in transit

All public-facing networks or traffic from public networks arriving at the public subnets should be encrypted using protocols such as HTTPS, or sftp

Use of firewall

Firewalls are defined as security systems that control and restrict network connectivity and network services. Firewalls establish a control point where access controls may be enforced. All connections from external and public networks should pass via a firewall. This requirement applies no matter the technology employed, including wireless connections, cloud networks, wifi-routers, etc.

Firewall rules

Firewall rules should, at the minimum, have the following protection

- OWASP top 10
- DDOS
- Block traffic from known malicious IP addresses
- Suspicious network activity
- Block specific ports and protocols

Firewall Access Mechanisms

Firewall access must be considered an elevated privilege and should follow procedures for granting elevated access.

Logging and Monitoring

All changes to network and firewall configuration parameters enabled services and permitted connectivity paths must be logged. All suspicious activity should be monitored using automated software. The integrity of these logs must be protected with checksums, digital signatures, encryption, or similar measures. These logs must be promptly removed and stored in a physically protected container for at least six months after the time they were recorded. These logs must be reviewed periodically to ensure that the firewalls operate securely.

Intrusion Detection

All firewalls must include intrusion detection systems. Each of these intrusion detection systems must be configured to identify potential problems like unauthorized modifications to firewall system files and detect denial of service attacks in progress, etc.

Backup of configuration files

Back-up copies of firewall and other network configuration files, connectivity permission files, etc., are backed up and kept for 90 days.

The backup files are stored in an online encrypted vault or alternate processing systems.

Virus Screening and Content Screening

All networks and network components such as firewalls must be screened for viruses or malicious code and files.

Virtual Private Networks

All remote and on-field employees should connect to VPN to access corporate networks. To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic, except Internet mail and other cloud-hosted systems, must be authenticated and encrypted with a VPN.

Network and firewall testing

- Because firewalls provide such an important control, their strength and proper configuration must be tested regularly. This testing process must include consideration of defined configuration parameters, enabled services, permitted connectivity paths, current administrative practices, and adequacy of the deployed security measures. These tests must include the regular execution of vulnerability identification software and the regular performance of penetration tests. These tests must be performed by technically proficient persons, either in the Information Technology department or working for a third-party contractor. Those responsible for either the administration or management of the involved firewalls must not perform these tests

Contingency Planning

Technical staff working on firewalls must prepare contingency plans that address the actions to be taken in the event of various problems, including system compromise, system malfunction, system crash, system overload, and Internet service provider unavailability. These contingency plans must be kept current and be created along with Incident Response Team and IT support teams.

Mapping with Industry Standards

This policy addresses the following risks related to Network management and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Malware	8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks 8.23 web filtering C 10.1 Continual improvement
Loss of CIA (Confidentiality, Integrity and Availability)	8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks 8.23 web filtering C 10.1 Continual improvement
Unauthorized access	8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks 8.23 web filtering C 10.1 Continual improvement
Information Leakage	8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks 8.23 web filtering C 10.1 Continual improvement
Data Breach	8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks 8.23 web filtering

Risk	Mapping to ISO 27001:2022
	C 10.1 Continual improvement

Enforcement

Departures from this policy will be permitted only if approved in advance and written by the IT department.

In some instances, systems such as routers or gateways may function as firewalls using Cloud-provided infrastructure.

Non- Compliance

Violations of the policy may subject employees to disciplinary action, including removal of privilege to the systems, up to and including termination of employment. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable Veranda learning policies.
- Termination of employment.
- Legal action according to applicable laws and contractual agreements.

Validity and Document Management

The owner of this document is the management, who must check and, if necessary, update the document at least once every 12 months.