

Synoligo Network Access Control Policy

Purpose

The purpose of this policy is to define the requirements for network access control (NAC) in order to protect the confidentiality, integrity, and availability of the organization's information assets.

Scope

This policy applies to all users of the organization's network, including employees, contractors, and guests.

Policy

The organization's NAC policy will include the following requirements:

All users must authenticate and authorize themselves before being granted access to the network.

All devices connecting to the network must be compliant with the organization's security policies.

The organization will use a NAC solution to detect and remediate non-compliant devices.

The organization will use a NAC solution to quarantine any devices that pose a security risk.

The organization will use a NAC solution to track network usage and identify suspicious activity.

Procedures

The organization's NAC policy will be implemented in accordance with the following procedures:

All users will be required to create a unique username and password for accessing the network.

All devices connecting to the network will be required to have antivirus software installed and up-to-date.

The organization's NAC solution will be configured to detect and remediate non-compliant devices.

The organization's NAC solution will be configured to quarantine any devices that pose a security risk.

The organization's NAC solution will be configured to track network usage and identify suspicious activity.

Responsibilities

The following individuals are responsible for the implementation and enforcement of the organization's NAC policy:

The Chief Information Officer (CIO) or equivalent is responsible for overall responsibility for the NAC policy.

The IT Security Manager is responsible for the day-to-day implementation and enforcement of the NAC policy.

All users are responsible for complying with the NAC policy.

Enforcement

Violations of the organization's NAC policy may result in disciplinary action, up to and including termination of employment.

Review

The organization's NAC policy will be reviewed annually to ensure that it remains effective in protecting the confidentiality, integrity, and availability of the organization's information assets.



Xibo Li

CEO

January 2023