Otero Home Network Policy

Last Reviewed Dec 23, 2024

Overview

The Otero family is committed to maintaining a safe, secure and reliable home network. The intentions of this policy are not to impose restrictions that are contrary to our values of openness, trust and transparency. Effective security is a team effort involving all family members to protect against cyber threats.

Purpose

This policy establishes the framework for securing the Otero home network and associated devices. Following it protects our personal data and prevents unauthorized access to our network.

Scope

This policy applies to all household members, guests, and any devices connected to the Otero home network. It encompasses all networked devices including, but not limited to, computers, mobile devices, smart appliances, and home automation systems.

Policy

4.1 Access Control

Network access is limited to authorized users.
Starting at time of account creation or device installation (routers, printers, etc), reputable password managers (installed on multiple devices to avoid single points of failure) will be used to produce strong passwords are required for all devices, including a mix of symbols, numbers, and case-sensitive letters, with a minimum length of 10 characters.
WPA3 encryption will be utilized to enhance wireless network security.

4.2 Awareness and Training

Click with caution! Regular meetings will be held to train household members on cybersecurity best practices such as password security, phishing awareness, and safe browsing habits.

4.3 Identification and Authentication

New devices must be manually added to the network to prevent unauthorized access.
MFA everyday! Online accounts will have MFA on authenticator apps or hard tokens, following a 3-2-1 backups rule (3 copies, 2 media, 1 copy offsite - e.g in a fire safe)

4.4 Security Assessment and Authorization

The network will be monitored for unusual activity, with specific measures to identify and block potential security threats.

4.5 System and Communications Protection

You've got to patch it! Update software regularly.

Protective measures against common cyber-attacks like DoS will be implemented.

Policy Compliance

Non-compliance may result in restricted network access. It is the responsibility of each user to adhere to this policy.

Last Reviewed Dec 23, 2024