OZARK REGIONAL LIBRARY

Library Internet Security Overview

1. Introduction

This document provides a detailed overview of the security measures in place to protect the library's internet connection. Our goal is to ensure a safe and secure online environment for all patrons and staff.

2. Security Measures

2.1 Antivirus Software

- **What is antivirus software?**
  - Antivirus software is a program designed to detect, prevent, and remove malware and other malicious software from computer systems.
  - It provides real-time protection and regular scans to ensure devices remain secure.
- **Implementation**
  - All library computers are equipped with antivirus software that is regularly updated.
  - The software is configured to perform daily scans and automatically remove any detected threats.
  - Patrons and staff are educated on best practices to avoid malware infections, such as not downloading untrusted files or clicking on suspicious links.

2.2 Physical Firewall

- **What is a Physical Firewall?**
  - A physical firewall is a hardware device that filters incoming and outgoing network traffic based on security rules.
  - It serves as a barrier between the internal network and external threats.
- **Implementation**
  - The library's internet connection is safeguarded by a physical firewall device.
  - The firewall is configured with security policies that block unauthorized access attempts and potential threats.
  - Regular updates and maintenance are performed to ensure the firewall remains effective against new vulnerabilities.

2.3 WPA2 Encryption

- **What is WPA2?**
  - WPA2 (Wi-Fi Protected Access 2) is a security protocol that provides data protection for wireless networks.

    - It uses Advanced Encryption Standard (AES), which is highly secure and widely recognized.
- **Implementation**
    - All library wireless access points are configured to use WPA2 encryption.
    - Users must authenticate with a secure password to gain access to the network.
    - Regular password updates and complex password requirements are enforced to maintain security.

2.4 Web Filters

- **What are web filters?**
    - Web filters are software or hardware tools that restrict access to certain websites and online content.
    - They help protect users from harmful or inappropriate material.
- **Implementation**
    - The library uses web filtering software to control and monitor internet access.
    - Categories of restricted content include malware, phishing sites, explicit material, and other inappropriate content.
    - Custom rules can be set to block specific URLs or keywords.

3. Conclusion

The library takes reasonable cybersecurity measures to safeguard information, including protected personally identifiable information (PII) and other types of sensitive data. This includes information designated as sensitive by federal agencies or pass-through entities, as well as information that the recipient or subrecipient considers sensitive. These measures are in compliance with applicable federal, state, local, and tribal laws concerning privacy and confidentiality.

The library is committed to maintaining a secure and safe internet connection for all users. To ensure robust protection against potential threats, we use antivirus software, a physical firewall, WPA2 encryption, and web filters. Regular updates and security audits are performed to continuously enhance our security measures.