Information Security Policy

The Umatilla County Special Library District (UCSLD) seeks to ensure that appropriate measures are implemented to protect customer and employee personal and sensitive information. This Information Security Policy is designed to establish a foundation for a UCSLD culture of security.

The purpose of this policy is to clearly communicate the UCSLD's security objectives and guidelines to minimize the risk of internal and external threats.

Compliance

Non-compliance with this policy may pose risk to the UCSLD; accordingly, compliance with this program is mandatory. Failure to comply may result in disciplinary action up to and including termination of employment – please see the UCSLD Discipline Personnel Policy. Management reserves the right to monitor, consistent with applicable laws, all activities within their business environment. The UCSLD will appropriately report violations of State and/or Federal laws and will cooperate with regulatory bodies and law enforcement agencies investigating such incidents.

Privileged Access

Access to the UCSLD's systems and applications above and beyond general user access shall be limited to the District Director and/or their designee.

Data Backup & Recovery

The UCSLD will conduct regular backups of all critical business data. Full data backups will be performed on a weekly basis. Checklist of backup information will be reviewed by the District Director periodically, but not less than monthly.

Multi-factor Authentication

Multi-factor authentication is highly suggested and will be utilized where most appropriate and when available.

Endpoint Protection

All UCSLD workstations will utilize an endpoint protection tool to protect systems against malware and viruses.

Firewall with Security Services

The UCSLD will protect their computers from the Internet through the use of a firewall with Intrusion Prevention System (IPS) capability.

Email Security

The UCSLD will protect their email system by utilizing antivirus, antispam and anti-phishing technologies. The UCSLD will also not utilize email to send or receive sensitive information.

Wireless

The UCSLD's wireless system is limited to staff and Board of Directors use only. The password will be changed yearly.

Password Management
The UCSLD will use a password configuration system. Current best practices will be consulted and will be available through the cybersecurity procedure and checklist. In addition, the UCSLD will educate users on creating/ utilizing secure passwords for systems/ services that can't be controlled by the UCSLD.

Security Awareness Training
The UCSLD's personnel are required to participate in security training in the following instances:

1. All new hires are required to complete security awareness training before being granted system access
2. The UCSLD staff will continue to share at monthly safety and staff meetings, new security issues, cybersecurity occurrences, best practices and training to expand security knowledge.
3. A formal refresher training is conducted on an annual basis. All employees are required to participate in and complete this training.

Acceptable Use Policy
The UCSLD will require all users sign an acceptable use policy before accessing UCSLD resources. This policy governs the use of the company resources and covers a wide range of issues surrounding the rights, responsibilities, and privileges – as well as sanctions – connected with computer use.

Asset Management
An inventory of all the UCSLD's hardware and software will be maintained that documents the following:

- Employee in possession of the hardware or software
- Location of hardware or software
- Date of purchase
- Serial number
- Type of device and description

Patch Management
All software and operating system updates and patches will be configured to automatically install. Periodic review will be conducted to ensure all updates and patches are applied to all devices.

Securing Remote Workers
The UCSLD requires all remote users to utilize company owned devices when working remotely. Those devices will be setup with a secure VPN.

Mobile Device Management (MDM)
The UCSLD will utilize a tool or service for the administration of mobile devices in the event the mobile device is used to access UCSLD information (this includes email).

Standard Configuration
The UCSLD will utilize a standard configuration for all endpoints, mobile devices, and printers. Any changes to the standard configurations will be reviewed and approved by leadership.

Vulnerability Scanning
The UCSLD will ensure all critical external and internal resources have periodic vulnerability scans conducted on them to ensure they are properly configured and updated.

Incident Response
The UCSLD will utilize an incident response plan in the event of cyber related incident. This plan will include at the minimum:

- Essential contact for an incident response service provider, FBI, local law enforcement, cyber insurance company, legal counsel.
- Users' roles and responsibilities.

Auditing and Logging
The UCSLD will ensure proper logging is enabled on all critical resources. At a minimum the following events will be recorded:

- Invalid Login Attempts
- Creation of New User Accounts
- Escalation of User Privileges