Appendix A – Acceptable Use Policy

Purpose
The purpose of this policy is to outline the acceptable use of computer equipment, email, and internet access at the Umatilla County Special Library District (UCSLD). These rules are in place to protect the employee and the company. Inappropriate use exposes the company to risks including virus attacks, compromises of network systems and services, and legal issues.

Scope
This policy applies to both permanent, temporary employees and volunteers of the UCSLD. This policy applies to all equipment that is owned or leased by the company. This policy is a supplement to the UCSLD Information Security Policy.

General Use
IDs/Passwords:
Access to the UCSLD's IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords to equipment are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on UCSLD systems and services.

Password Requirements:
- Minimum password length: 10
- Must have a combination of letters, numbers, and special characters.
- If possible, utilize a password manager to create (much stronger) and unique passwords for each service or account.

Individuals must not:
- Allow anyone else to use their user ID and/or password on any UCSLD IT systems.
    - Exceptions to this must be approved by District Director or their designee.
- Leave their password unprotected.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Perform any unauthorized changes to the UCSLD's IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Insert unapproved media (CD, USB thumb drive, SD card) into UCSLD devices.
- Store UCSLD data on any non-authorized equipment, or personnel equipment.
- Give or transfer UCSLD data or software to any person or organization outside of the UCSLD without the authority of the District Director or their designee.

Internet and Email Use
Use of the internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the UCSLD in any way, not in breach of any term and condition of employment and does not place the individual or UCSLD in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems. Individuals must not:

- Disclose employee, client, and other proprietary information which the employee has access.
- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which the UCSLD considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to the UCSLD, alter any information about it, or express any opinion about the UCSLD, unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Forward UCSLD mail to personal non-UCSLD email accounts (for example a personal Gmail account).
- Make official commitments through the internet or email on behalf of the UCSLD unless authorized to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval.
- Remove or disable anti-virus software.
- Use unauthorized services on the internet to store or transmit PII (personally identifying information). This includes (Dropbox, Google Drive, personal email accounts, etc.)

Email:
To avoid being a victim of malicious software or phishing attack remember:

- Never download or open attachments from unknown recipients.
- Hover over links to determine if the link is legitimate.
- If it's a specific account asking you to sign into an account don't click a link within the email visit the site directly to login.
- Verify sender. Sometimes the best way to do this is call the sender back to make sure they are the ones who initiated the email.
- Never provide personal information. Legitimate companies will never ask for you to provide personal information including passwords in an email.

Clean Desk and Clear Screen
In order to reduce the risk of unauthorized access or loss of information, the UCSLD enforces a clear desk and screen policy as follows:

- Maintaining a “clean desk” or working area throughout the day and ensure there are no confidential documents in open view if absent from their desk for an extended period of time. This will help to ensure that confidential customer information is not inadvertently disclosed.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Ensure that paper-based information is appropriately monitored and protected.
- Ensure that all confidential documents are properly locked-up at the end of each business day. Appropriate methods to secure documents include utilizing locking filing cabinets or desk drawers, etc.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site
It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Only equipment approved by the UCSLD may be used to download personal information locally to the device.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car. Lock devices in the trunk out of sight while traveling.
- Laptops must be carried as hand luggage when traveling.
- When outside the office, computers must utilize the endpoint protection VPN before connecting to resources.

Mobile Devices

- Mobile devices such as smartphones and tablets may be used but require approval.
- It is not permitted to save client information locally to a mobile device.
- Mobile devices need to be password protected.

Mobile Storage Devices
Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only authorized mobile storage devices ~~with encryption enabled~~ must be used, when transferring sensitive or confidential data.

Telephone Equipment Conditions of Use
The use of UCSLD voice equipment is intended for business use. Personal use of voice equipment is allowed but should be limited. Individuals must not:

- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

Actions upon Termination of Contract
All UCSLD equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the UCSLD at termination of employment.

Monitoring and Filtering
All data that is created and stored on UCSLD-owned computers and third-party vendor's systems is the property of the UCSLD and there is no official provision for individual data privacy, however wherever possible the UCSLD will avoid opening personal emails.

System logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The UCSLD has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

It is your responsibility to report suspected breaches of security policy without delay to the District Director. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the UCSLD's disciplinary procedures.

Signature
I have received a copy of the UCSLD's Acceptable Use Policy as revised and approved by the management. I have read and understand the policy.

_____
(Print your name)

_____ _____
(Signature) (Date)