YAKIMA VALLEY LIBRARIES

In the Matter of:
Yakima Valley Libraries
Information Technology Policy

RESOLUTION
# 14-006

WHEREAS, the Trustees of Yakima Valley Libraries review and establish policies as appropriate;

WHEREAS, there is a need to establish an Information Technology Policy for Yakima Valley Libraries:

WHEREAS, the Board of Trustees have completed a first reading and second reading and review of the policy;

BE IT THEREFORE RESOLVED, that the Yakima Valley Libraries Information Technology Policy be approved by the Board of Trustees.

ADOPTED BY THE BOARD OF TRUSTEES this 27th day of October, 2014.

Trustee

Trustee

Trustee

Trustee

Trustee

YAKIMA VALLEY LIBRARIES' POLICY ON INFORMATION TECHNOLOGY AND USE OF RESOURCES

TABLE OF CONTENTS

1. General

A. **General Policy:** Trustees, Management, Managing Librarians, Department Heads supervisors, and employees are obligated to conserve and protect Library resources for the benefit of the public interest, rather than their private interests. Employees of Yakima Valley Libraries are public employees subject to the laws of the State of Washington.

Responsibility and accountability for the appropriate use of Library resources ultimately rests with the Trustees, the Library Director and Library Managers who use Library resources or who authorize such use.

All technology, except as specifically excluded in writing by the Trustees or Library Director, will be vetted and sanctioned by the Library Director or his/her designee. This includes operations, maintenance, purchases, system development, contracting for services and all other functions regarding technology, regardless of the department or agency that will employ it.

B. **Privacy:** Yakima Valley Libraries is subject to RCW 42.56. The Public Records Act considers most records generated by a public agency, such as the Yakima Valley Libraries, to be public and subject to disclosure, unless specifically exempted in this statute. Users (staff) shall have no expectation of privacy when using any technology system, equipment or device that is used to access Yakima Valley Libraries' resources. This includes use of any access for official Library business or an allowed personal use as provided herein.

An exemption for Library privacy is outlined in RCW 42.56.310 –

> "*Any library record, the primary purpose of which is to maintain control of library materials, or to gain access to information, that discloses or could be used to disclose the identity of a library user is exempt from disclosure under this chapter.*"

This applies to protected library user information in the YVL integrated library system to which staff may have access.

By using the Library's technology system and resources, with the exceptions listed, employees acknowledge and agree that they have no expectation of privacy or confidentiality in their use of the system or in any data that they create, store, or transmit on or over the system, including any data created, stored or transmitted during the employees' incidental personal use of the computer system as permitted under this policy.

Employees who use the computer system further agree that they are aware of, understand and will comply with the provisions of this policy, and that their use of the computer system may be monitored and any data that they create, store, or transmit on or over the system including incidental personal use of the computer as permitted by the policy (or the creation of Library data on personal devices), may be inspected by the Library at any time. In addition, email messages, text messages, telephone messages, and other documents created on the Library technology systems are public records and may be subject to public disclosure.

C. **Definitions:** As used in this policy:

1. ***Library*** means Yakima Valley Libraries (YVL), unless otherwise specified. All references to specific departments are to Yakima Valley Libraries' Departments or Community Libraries unless otherwise specified.

2. ***Library resources*** includes any information, data, money, service, software, equipment or other property or resource under the officer's or employee's official control or direction or in his or her custody or to which he or she has access.

3. ***De minimis* cost** means that the actual expenditure of Library funds is so small as to be insignificant or negligible. *De minimus* shall not be applied to the cost of property which is consumable, such as paper, envelopes or spare parts, even if the actual cost to the Library is insignificant or negligible – such costs must be reimbursed or not incurred.

4. ***Electronic mail*** also called ***email*** means the transmission of memos, messages and files over an automated, networked system. Electronic mail includes storing and forwarding capabilities and the user interface.

Electronic mail includes mail sent or received on the Yakima Valley Libraries' computer network, the Internet, and any other network.

5. ***Forwarding of email*** means the ability to transmit email messages addressed to a specific party or parties to another party over the network.

6. ***Internet*** means the thousands of interconnected networks originally developed by the military and referred to as the Internet, the Information Super Highway, the Net, or similar names.

7. ***Management, Library Director, Department Head, Managing Librarian, Manager, Supervisor, Staff, or Employee*** means Yakima Valley Libraries' staff unless otherwise specified.

   Trustee means a member of the Board of Trustees who has been officially appointed by the Yakima County Commissioners.

8. ***Social Media*** means a set of Internet tools enabling users to participate in community experiences online and to connect with people of common interests to learn, play, work, organize, and socialize; networks may be open to the public or restricted to members as determined by the user. Social media includes, but is not limited to, blogs, Facebook, Flickr, Twitter, and YouTube.

9. ***Media*** is digital media that are encoded in a machine readable format: information or data that can be created, viewed, modified, and preserved on computers.

10. ***Library Devices*** are personal computers, laptops, hybrids, tablets, cell phones or other library equipment assigned to staff for the performance of their job duties.

11. ***IT Department*** is Yakima Valley Libraries' Information Technology Department.

D. **Implementation:** This policy shall be effective immediately upon adoption and shall supersede all policies previously adopted by the Yakima Valley Libraries' Trustees with regard to use of Library resources or property.

E. Nothing in this policy is intended to limit the ability of the Trustees or Library Director to adopt policies or procedures that are more restrictive than the prohibitions provided herein.

2. Access and User Management

A. **General Policy:** This provision defines requirements for managing user (staff) accounts, authentication information, and access control systems for Yakima Valley Libraries.

B. **User IDs – Email:** Unique User IDs for email and access to the integrated library system (or others as designated) will be created and assigned to each individual requiring access to Yakima Valley Libraries information resources. *This email identification belongs to the Library and may only be used to access Library related activities and may not be used for personal login information.*

C. **Privileges:** Access rights to privileged User IDs are restricted to the least privilege necessary to perform job responsibilities. Assignment of privileges is based on individual person's job classification and function. Access to all information assets shall only be granted based on need-to-know, right-to-know, and time-to-know.

D. **Assignment of User ID:** Everyone requesting a User ID will have a request form signed by the management with their privileges listed. User IDs shall only be created and assigned to users through a formal process that requires approvals.

E. **Accountability:** Upon receiving a User ID, the owner will be individually accountable for how it is used.

F. **Audit:** The IT Manager or authorized designee shall be responsible for periodically (at least biannually) reviewing user access rights to information systems to verify that access rights are appropriate.

G. **Strong Passwords:** Passwords and their expiration shall conform to best practices for technology requirements.

1. Personnel responsible for resetting passwords shall positively identify users who request password resets prior to resetting the password.

2. Any time the password is reset by someone other than the user, the user shall be required to change his/her password before continuing.

3. Users shall promptly change all passwords if they are suspect of being, or known to have been, disclosed to unauthorized parties.

4. First time passwords for new users must be set to a unique value for each user; the user shall be required to change his/her password before gaining access into the Yakima Valley Libraries' environment.

5. Accounts for terminated users shall be immediately removed or inactivated. In certain cases, the Director may ask that the terminated employee's access be rerouted to a supervisor or manager for review of YVL related information.

6. Accounts used by vendors for support and maintenance purposes shall only be enabled when needed, and monitored while in use. Once vendor maintenance has been completed, the account shall be disabled if possible. If account disablement is impossible, the password should be reset to a random alphanumeric string and the event documented.

7. Shared or generic User-IDs and passwords are explicitly prohibited unless approved in writing by Director and/or designee.

8. Where possible user accounts should be locked out after six logon failures. Lockout duration should be set to thirty minutes or less or until system administrator resets the account.

9. Where possible, automatic screen locks and/or session timeouts should function after no more than 15 minutes of being idle on any Library resource that can access sensitive information.

10. Passwords shall be changed whenever a compromise is suspected and documented.

11. System administrators should not use privileged accounts unless it is the only option available. Unique login IDs for System Administrators are preferred for regular tasks and maintenance.

12. Automatic system requests for regular password changes will be implemented where possible.

3. Use of Library Systems

A. **General Policy:** The Library's technology systems are provided to assist employees to perform their jobs, share files, and communicate with each other and with outside individuals and organizations on Library business. The Library's technology systems are to be used for Library business purposes, exception for occasional, incidental personal use as permitted consistent with the guidelines below.

B. **Appropriate Use:** The Library's computer systems are to be used by employees, Trustees, or volunteers for Library business.

The technology systems may also be utilized for occasional, incidental personal use that, in the judgment of the employee's supervisor or manager, does not interfere with employee or department productivity. Personal use does not include uses requiring substantial expenditures of time, uses for profit, or uses that would otherwise violate Library policy with regard to employee time commitments or Library equipment.

Examples of acceptable occasional, incidental personal use of the Library technology system may include:

1. Advising others about an employee's vacation, marriage, birth of child, etc.

2. Brief and infrequent communication.

3. Important and time sensitive personal needs such as making medical appointments or arranging parent-teacher conferences.

4. Personal use of impact similar to that of a brief phone call.

5. Browsing on-line edition of newspaper or websites during lunch or break time.

C. **Examples of Inappropriate Use:** Use of the Library's technology system to engage in any communication or act that violates federal, state, or local laws, codes, regulations, or Library policies and procedures is strictly prohibited at all times. Inappropriate uses of the Library's technology include, but are not limited to:

1. Commercial use for an employee's personal business.

2. Usage for any type of harassment or discrimination.

3. Usage for any activity that could adversely affect the Library's image or reputation.

4. Usage which violates software license agreements.

5. Downloading of software for personal use.

6. Unauthorized entry or attempt of entry into other Library department's sub-directories, files, resources, or

7. Malicious use of the system in an excessive manner so as to unreasonably deprive others of system use or resources.

4. Library Staff Computers, Laptops, or other Devices

A. **General Policy:** It is the policy of Yakima Valley Libraries to provide reliable, secure, and adequate personal computing platforms – Library Devices – (PCs, laptops, or other devices). These Library Devices shall be the property of Yakima Valley Libraries, have adequate virus and malware protection, and provide for network connectivity if applicable.

B. **Purpose:** Computers are provided for Yakima Valley Libraries work and are subject to audit at any time.

1. There shall be no **expectation of privacy** regarding use or storage on a Library Device.

2. Library Devices may be accessed at any time, without notice, over the Library network for business purposes when authorized by Library Director. In normal circumstances, attempts will be made to notify employee before accessing staff computer.

4. All work files shall be stored in a location as designated by the Director or IT Manager. Only *copies* of work files may be stored on the local hard drive of any PC unless otherwise approved by the Director. No staff may store work files (original or copies) off site without prior permission of the Library Director.

5. Adequate storage shall be provided for work products.

6. Library devices may be used for *de minimus* personal use by employees at appropriate times.

7. Library devices may not be used for any prohibited activities as stated in section 3.C of this policy.

5. Electronic Mail and Text Messaging

A. **General Policy:** Electronic mail is an integral part of Yakima Valley Libraries communications. It is the policy of Yakima Valley Libraries to encourage the responsible use of electronic mail whether internally or externally generated or viewed. This policy is meant to make all users aware of the risks associated with using electronic mail and to inform them of Yakima Valley Libraries' policy regarding such use. This policy applies to the electronic version of the messages and any paper or printed copies of the messages.

B. **Purpose.** The primary purpose of Yakima Valley Libraries' electronic mail system is to facilitate the timely and efficient conduct of Library business. The system is also provided to encourage and facilitate the free exchange of business-related communications and ideas between employees.

C. **Right of Inspection.** The electronic mail system is intended for business purposes. Electronic mail communications constitute public records and the Library has the right to access or monitor messages for work-related purposes, security, or to respond to public records requests. All messages should be composed with the expectation that they are public. **Users shall have no expectation of privacy in email messages, whether they are business related or an allowed personal use as provided herein.** Use of electronic mail shall be considered consent to Yakima Valley Libraries' Director or his/her designee to inspect, use or disclose any electronic mail or other electronic communications and/or data without further notice.

D. **Prohibition of Inappropriate Message Contents.** Electronic mail should be business like, courteous and civil. All Yakima Valley Libraries' policies, including policies prohibiting discrimination and sexual harassment, shall apply to use of email and messaging. Email shall not be used for the expression of unlawful or discriminatory ill-will or bias against individuals or groups.

E. **Forwarding of Electronic Mail.** A user forwarding a message which originates from someone else should not change the substance of the message without disclosing what you have changed. Some changes do not need to be disclosed, such as deleting extra spaces or lines, lists of recipients of the email (except where that is relevant), or duplications of the same message within the email.

F. **Mis-delivered Messages.** If an electronic mail message comes to a user by mistake, the user should stop reading as soon as he or she realizes that the message was not meant for him or her and notify the sender or system administrator immediately.

G. **User's Responsibility for Security.** Users are responsible for the security of his/her electronic mail account password and any electronic mail that is sent via a user account. To protect a user account against unauthorized use, the following precautions should be taken:

1. ***Lock your PC or log off*** from the Library network before leaving computer unattended. If user ID logon is left open, and someone else uses it, it will appear as if user sent the message and user will be held accountable.

2. ***Do not give out passwords.*** Users are responsible for messages sent via user account. Correspondingly, do not use or tamper with someone else's account without his/her knowledge and consent. Unauthorized use of an electronic mail account is in violation of this policy.

   If you believe your passwords have been compromised, please notify your supervisor and change immediately.

3. ***Your Library email address may only be used for Library related identification.*** It should not be used as a user-name for unrelated Library access.

H. **Text Messaging.** This mode of communication is to be used in terms of urgent need or to communicate quick informal information. At all times it is important to ensure communication is received and understood. There is no guarantee a text message will be received. All text messages are subject to public disclosure and are retained as per the Library's retention schedule.

6. Internet Access

A. **General Policy:** It is the policy of Yakima Valley Libraries to encourage effective and efficient use of all Library equipment for completion of Library business. This includes use of the Internet to provide information to Library patrons, businesses and other governmental agencies to search for information, and for information exchange as expected for the provision of library services.

B. **Personal Use:** Internet access is provided for Library business purposes.

Exceptions for personal use are provided in section 3.B of this policy. Any personal use on a Library Device may be subject to a Public Records Request. There is no expectation of privacy for personal use on a non-public library device. **Staff use of a public library computer as a member of the public is protected information.**

C. **Libraries provide access to information.** Within its mission and objectives, Yakima Valley Libraries provides open access to information that best supports the needs of Library users. Yakima Valley Libraries provides access to information without bias. There may be times when information that appears objectionable to some may need to be be accessed to best support and serve the needs of the users. This is within the scope and mission of the Library. Staff must use discretion and judgment when using staff computers for research.

D. **Access reporting and monitoring:** It is the responsibility of the Manager or Supervisor to monitor and be aware of use of the Internet within the department.

E. **Copying Files:** Files copied from the Internet, or any other outside service, should be for Library purposes and must be scanned by a virus checking software prior to being used on a Library computer. Yakima Valley Libraries Technology Services shall make options available for virus checking of copied files.

F. **Distributing Files:** Caution should be used with distribution of Library files via the Internet. Files distributed to the Internet have the possibility of being intercepted by others and used against the Library's interest. Files are not to be distributed to the Internet without the express consent of the employee's Manager, Supervisor, IT Manager, or Library Director.

G. **Privacy:** The Library reserves the right to monitor the activities of all Library employees' access of the Internet. **Users shall have no expectation of privacy in accessing the Internet using Library resources, whether that access is business related or an allowed personal use as provided herein.**

7. Social Media

A. **General Policy:** All official Yakima Valley Libraries' presences on social media sites or services are considered an extension of the Library's information and communications networks. Personal presences on social media, held by Library employees, should not infer or imply that they are official, speak on behalf of the Library Director in any way or utilize any recognizable Library logo(s). Exceptions for personal use are provided in section 3.B of this policy. There is no expectation of privacy for personal use on an assigned Library Device (computer).

B. **Guidelines:** Use of social media will comply with the following:

1. Unless otherwise approved by the YVL Library Director his/her designee, content posted to a social media site will be posted to an official Yakima Valley Libraries' Website(s).

2. All social media content shall be considered a secondary copy as approved above and contain references to primary content on the Library's official web site unless otherwise approved by the Director or his/her designee.

3. All Library use of social media must be in compliance with this policy.

4. All libraries will be represented by one designated account per social media type unless expressly approved by the YVL Library Director.

5. The YVL Director his/her designee will review and approve requests to use social media sites.

6. Use of social media must comply with applicable federal, state, and county ordinances, regulations, and policies, as well as proper business etiquette. This includes adherence to established laws and policies regarding copyright, records retention, release of public information, constitutionally protected freedom of speech, privacy laws and information security policies established by Yakima Valley Libraries.

7. Employees representing Yakima Valley Libraries via the Library's social media outlets must conduct themselves at all times as representatives of Yakima Valley Libraries with message and branding consistent with the policies of Yakima Valley Libraries. Employees who fail to conduct themselves in an appropriate manner shall be subject to the disciplinary procedures outlined in Yakima Valley Libraries Personnel Policy.

8. Violation of these standards may result in the removal of pages from social media outlets. The Yakima Valley Libraries' Trustees and the Director retain the authority to remove any or all violating information.

9. Yakima Valley Libraries reserves the right to remove any messages or postings they deem as inappropriate, including but limited to those that are:
   - Obscene
   - Profane
   - Sexual content or links to sexual content
   - In violation of the copyright, trademark right, or other intellectual property right of any third party
   - Not topically related to a particular social media thread
   - Repetitive or spam
   - In support or opposition to political campaigns of any kind
   - In support or that promotes, fosters or perpetuates discrimination of any kind
   - A solicitation of commerce
   - Illegal or encourage illegal activity

C. **Procedures:** The following procedures apply to the creation and setup of each official Library social media website.

1. Departments or community libraries requesting to distribute information on Yakima Valley Libraries' official social media pages via the Community Libraries Resource Manager will coordinate to develop a request for service.

2. Requests for social media will be reviewed and approved by YVL Library Director or designee.

3. If approved, the Community Libraries Resource Manager will be responsible for creating and maintaining all social media constructs.

4. Only Yakima Valley Libraries' e-mail addresses or e-mails authorized in advance by the Director will be posted on the site or used to create the

web site accounts. Use of generic email addresses, for example, webmaster@yvl.org, is appropriate to create social networking accounts.

5. To the extent that design parameters of the host site allows, Yakima Valley Libraries' pages will conform to the following:
   - Be identified as a Yakima Valley Libraries' official site,
   - Contain appropriate staff contact information,
   - Contain an easily identifiable Library logo,
   - Have a link to the appropriate page of the Library's website, and
   - Specify that all content, comments, and replies posted will be subject to Washington state and federal information laws.

6. YVL-generated content shall:
   - Comply with all guidelines and requirements of this section.
   - Contain the following legal disclaimer:

     "Yakima Valley Libraries is not responsible for the content nor endorses any site which has a link from or to this page. All content, comments and replies posted are subject to Washington state and federal laws. Yakima Valley Libraries reserves the right to remove any messages or postings in violation of state and federal law or county policy."

8. Contracting and Third Party Access

A. **General Policy:** These provisions identify the requirements related to information security for third parties working on behalf of or in association with Yakima Valley Libraries. These requirements also apply when providing third party access to Yakima Valley Libraries' information systems that store, transmit, or process confidential information. Where applicable, these requirements should be reflected within contracts when contracting with: (A) third parties who may obtain, create, receive, maintain or transmit confidential information on behalf of Yakima Valley Libraries, and (B) third parties who have access to Yakima Valley Libraries' information systems that store, transmit, or process confidential information.

B. **Access Control:** YVL Technology Department is responsible for maintaining a list of all connected entities that physically or logically have access to Yakima Valley Libraries production environment.

C. **Access audit and due diligence.** Prior to contracting and/or providing third party access to Yakima Valley Libraries' information systems, Yakima Valley Libraries shall perform due diligence, which may include audits, evaluations, test, reports, or other material to determine the third party's ability to protect critical services or confidential information.

D. **Payment Card Industry Compliance.** Third party shall be responsible for adherence to Payment Card Industry Data Security Standard requirements most recent version (PCI compliance).

E. **Non-disclosure and Confidentiality.** Applicable security requirements, including non-disclosure and confidentiality provisions, for third parties shall be included in written contracts when executed, modified or amended.

F. **Yakima Valley Libraries' Technology Standards.** Contracts shall require third parties and their subcontractors to adhere to Yakima Valley Libraries Information Security requirements, whether now or hereinafter in effect.

G. **Third Party Equipment.** Third party equipment used to access the Yakima Valley Libraries network shall be subject to review and approval prior to access being granted.

H. **Termination of connection.** Yakima Valley Libraries shall reserve the right to terminate a third party's contract for a material violation or breach of the security provisions. Further, Yakima Valley Libraries' contracts shall reserve the right to remove or terminate a third party's access to Yakima Valley Libraries' systems or facilities, without notice.

9. Non-Library Computing Facilities

A. **General Policy:** It is the policy of Yakima Valley Libraries to facilitate the most cost effective and efficient manner to do business while maintaining compliance with federal, state, and local laws and other requirements. Yakima Valley Libraries' data may be processed and stored in non-library facilities if approved by the Library Director. The Library Director or designee shall approve such a facility if it provides the most appropriate solution, is cost effective, and it follows the appropriate security standards.

B. **Definitions.** The following terms shall have the following meanings:

1. ***Offsite Storage is*** any facility that is used to store Library data that is not legally part of Yakima Valley Libraries and under the control of the Library District is deemed to be "offsite."

2. ***Offsite Computing Facility*** is any vendor or third party which provides services to Yakima Valley Libraries wherein computation takes place at the vendor or third party's facility.

3. ***Secure Computing Environment*** defines an environment that meets all federal, state and local security access, archive and backup standards as required by the type of data that is being processed.

4. ***Secure Background Check*** means a fingerprint background check that complies with federal and state standards.

5. ***Security Breach*** means any event that compromises the integrity of Yakima Valley Libraries' data. Integrity is compromised if data is read by an un-authorized individual, lost, stolen, amended, edited or any other event that exposes or alters information that would violate the federal, state or local statues that govern it.

C. **Usage Policy:** All computer systems contracts, leases, licenses, consulting arrangements or other agreements shall contain terms approved as to form Yakima Valley Libraries legal representative advising vendors of the Yakima Valley Libraries' retained proprietary rights and acquired rights with respect to its information systems, programs, and data and requirements for computer systems security. All such documents shall be approved by the Library Director.

D. **Responsible Party:** When using non-Yakima Valley Libraries' computing facilities to process or store data, the data owner has responsibility to ensure vendor compliance with appropriate Yakima Valley Libraries' policies and procedures. Appropriate secrecy protection agreements must be signed by the vendor providing the services.

E. **Vendor Requirements:** Vendors shall adhere to all the required federal, state and local requirements that apply to the type of data that they are processing, storing or backing up. If applicable, secure background checks shall be performed and copies of the background checks for each employee who will have the ability to access secure data shall be forwarded to Yakima Valley Libraries. Background checks shall be kept current based upon the applicable federal, state or local requirement.

1. Security breach of any kind shall be reported to the Library Director or designee as quickly as possible.

2. Vendor assumes all liability for security breach while Library data is in the vendor's possession or under their control.

3. Vendor shall allow onsite audit by Yakima Valley Libraries to ensure regulatory compliance. One working day will be sufficient notice to vendor and will be provided in writing via email or hard copy.

10. Networks and Security

A. **General Policy:** It is the policy of Yakima Valley Libraries to prevent unauthorized access to networks owned or operated by the Library and to maintain the integrity of the network by providing minimum requirements for network access control. All Library networks, regardless of use or purpose, will be managed and administered by YVL Technology Department or authorized vendor. For computing environments provided by third party service providers on behalf of Yakima Valley Libraries, corresponding contracts should reflect these requirements.

B. **Procedure:** Access Controls

1. Appropriate steps shall be taken to safeguard internal systems from untrusted networks, using methods such as Demilitarized Zones (DMZs) and firewalls.

2. Both inbound and outbound network traffic shall be controlled and limited to only that which is necessary to accomplish Yakima Valley Libraries' business objectives.

3. Access to or from untrusted networks shall be approved by the Library Director or designee prior to their implementation.

4. Connections to untrusted networks shall be implemented using connections methods approved and implemented by YVL Technology Department.

5. External access to diagnostic and administration connection points shall be physically and logically controlled.

6. Firewalls managed by Yakima Valley Libraries or authorized third party providers shall follow established rules as identified within supporting firewall configuration standards.

7. Any changes to a computing environment managed by a third party service provider shall be vetted with and approved by the Library Director or Technology Department designee prior to implementing a change.

8. YVL Technology Department will conduct a risk assessment prior to granting third party access to the Yakima Valley Libraries' network, data or information systems to ensure that no potential vulnerabilities are introduced due to such access. If an exposure is found, it will be mitigated by third party prior to being granted access. If no mitigation can be found, access will be denied.

9. Any potential risk associated with granting such access to a department's information shall be documented, and approved by YVL Library Director or designee as to their acceptance of risk.

C. **Procedure:** Device Access

1. Devices connected to the Yakima Valley Libraries' network and not approved by the Director or IT Manager shall be subject to immediate inspection, removal from the network, seizure, and retention by YVL IT Department for as long as necessary to accomplish the goals of this and other Library policies. These actions may be required by such issues as infection of malware, court order, departmental disciplinary actions etc. No expectation of privacy shall exist regarding any information on a connected device. Devices shall include but not be limited to: smart phones, tablets, thumb drives, external hard drives, SIMS, electronic cameras or any device that allows data to be transferred into or out of the Library network.

2. Third party devices may be granted access to the Yakima Valley Libraries network only by prior permission from the YVL Library Director or designee and will be granted only if deemed appropriate and reasonable by the Library Director.

3. Access devices which provide internal or external access to Yakima Valley Libraries' information systems such as modems, wireless access points, or similar technology shall not be deployed without the YVL Library Director's written approval.

4. All access to Yakima Valley Libraries' production environments that occurs through the above mentioned and similar technology must be authenticated to identify the entity connecting to the environment.

5. The YVL Technology Department is responsible for maintaining an updated list of all access devices that connect to the Library network, identifying the device, business justification, owner, and contact information.

6. Use of access devices for other than established Library business reasons is prohibited.

7. Access to productions systems via dial-in connections (modem) shall be

configured to disable the ability to copy personal credit card information onto the local hard drive or any other type of external media, and disable the ability to cut-and-paste or print any credit card information.

11. Monitoring System Access and Use

A. **General Policy:** In a reasonably secure network and computing environment, appropriate monitoring and auditing provide a level of accountability to ensure appropriate use of information resources by employees and third parties. It is the policy of Yakima Valley Libraries to monitor and audit user and system activity on all Yakima Valley Libraries' systems that allow the ability to directly access, store, process, or transmit business, confidential or proprietary data, as well as determining what should be monitored or audited, and protect audit logs.

B. **Procedure:** System Access, System Use Events and Audit Logging – Every computer system should:

1. Enable logging to record successful and unsuccessful attempts to read or modify an information resource that stores, transmits, or processes Confidential or Proprietary information or as deemed necessary by the Library Director.

2. Enable logging to record all actions taken by accounts having special system privileges.

3. Enable logging to record changes to the function for auditing including enabling, disabling, and access to auditing features.

4. Enable logging to record access to audit trails and initialization of audit logs.

5. Enable logging to record User login activity including successful and unsuccessful login attempts, User ID or identifier, and authentication mechanism and any system level objects.

6. Enable logging to record activities of User ID creation, deletion, and changes to User ID privileges.

7. For each logging record identified above

8. Wherever applicable, the system component shall be configured to capture:

   - User Identity (User ID or identifier)
   - Type of event/activity
   - Date and time
   - Success or Failure
   - Origination of event
   - Name of affected information resource (data, system component)

C. **Collection and Review of Audit Logs:**

1. Log consolidation and parsing tools shall be utilized to perform automatic daily review, and send alerts to authorized individual if suspicious or malicious activity is detected.

2. Audit logs shall also be reviewed on a periodic basis at least quarterly or as defined by YVL Library Director.

3. Audit logs shall be retained for a reasonable period of time or as defined by Electronic Data retention standard.

4. Evidence of log reviews shall be retained in accordance with Electronic Data retention requirements.

5. File integrity monitoring software will be used on all logs to ensure that existing log data cannot be changed without generating an alert.

D **Clock Synchronization:** Technology Services shall enable synchronization of system clocks through NTP or similar technology to ensure the consistency of time reporting in audit logs.

E. **Log Consolidation and Correlation:** Production system components logs shall be promptly backed up to a centralized log server or media. Production systems logs (OS, application, database), antivirus logs, network equipment logs, and

IDS/IPS devices logs shall be consolidated to a centralize LOG server or similar technology for consolidation and correlation of events.

12. Computer Equipment/Media Handling, Disposal, and Reuse

A. **General Policy:** It is the policy of Yakima Valley Libraries to protect confidential and sensitive data stored on various forms of computer media and equipment from unauthorized or accidental disclosure to persons who do not have a need to know or use this information. An important aspect of protecting confidential and sensitive information is to appropriately protect such information when it is being transported, transmitted, disposed of or reused.

B. **Procedure:** Media Handling and Security

1. All media contacting confidential data (E.g. PCI, HIPAA, CJIS or other sensitive data) will be labeled to ensure it is treated according to that label.

2. Electronic media that contains confidential information shall be appropriately protected using approved cryptographic methods.

3. No media containing confidential media shall be released to unauthorized parties for repair, disposal, or reuse, unless contracted to do so and the contract has language for protection of confidential data, and any such data will be logged, authorized by management and secured so that the delivery mechanism can be traced.

4. Portable/Removable media should not be used to store confidential information, unless unavoidable for business related functions. If removable media is used to store confidential data, a record of the media, the data and the personnel responsible for it, shall be created and the removable media shall be protected using approved cryptographic methods.

5. Personnel responsible for portable/removable media containing confidential data shall be accountable for its movements into, out of, and within a facility or off-site; and are responsible for protecting the confidentiality of the data on such media and reporting any loss, theft or unauthorized access immediately to the YVL Library Director as well as appropriate department management. IT personnel shall maintain a record in any legible format of the movement of such media if it is released from their control as identified above.

6. Media that does not contain confidential information may be disposed or reused as identified in the instructions above or media shall be re-imaged, overwritten or reformatted prior to re-assignment.

7. Media back-ups containing confidential information should be stored in a secure offsite location (Alternate/backup site or commercial storage facility).

8. Periodic inventories will be maintained as required by statute for all confidential data (E.g. PCI, HIPAA or other data).

C. **Computer Equipment/Media Disposal and Reuse:** Confidential information when no longer needed for legal, regulatory, or business reasons shall be disposed and/or conditioned for reuse. This statement applies to all media, regardless of form.

1. Disposal: When equipment containing confidential information is being destroyed, the media part of the equipment shall be disposed of as described according to the disposal instructions listed below. Once the media is removed and disposed of according to disposal instructions provided below, the equipment may be declared surplus, destroyed or donated according to Library policy. Acceptable methods of media disposal include:

   - incineration
   - shredding
   - pulverization

   If a third party destroys the media, the third party shall provide a certificate of destruction or a periodic report detailing the destruction services that the third party has performed during that period.

2. Reuse: When equipment containing confidential information is reused, the media part of the equipment shall be treated according to media reuse instructions listed below. When media will be reused, the data on the media shall be scrubbed using one of the following methods:
   - Overwriting – Data shall be overwritten using current DOD standards for secure data.
   - Degaussing – Exposing the media to a strong magnetic field in order to sanitize magnetic media.

13. Vulnerability Management and Threat Assessment

A. **General Policy:** It is the policy of Yakima Valley Libraries to have the YVL IT Department manage information security threats and mitigate vulnerabilities within reasonable business methods and practices.

B. **Procedure:** Standard practices shall include but not be limited to:

1. A vulnerability mitigation process shall exist for new and existing systems, and shall include monitoring of vendor and security-related alerts and patches.

2. Vulnerability risk assessments and resolutions shall be documented no less than annually.

3. System and network vulnerability management (such as installation of updates, patches, or fixes) shall be coordinated through a change management process.

4. All system components and software should have latest security patches installed, relevant security patches should be installed within one month of release unless the business system precludes their installation.

5. Both internal and external threats shall be identified and assessed as part of the risk analysis process.

6. If overall heightened awareness is warranted, appropriate personnel shall be notified of threats.

7. Internal and external network vulnerability scans must be conducted on periodic basis at least quarterly and after any significant change in the network as authorized by the YVL Library Director or designee.

8. Penetration tests (network and application) must be conducted at least once a year and after any significant change to the production environment as authorized by the YVL Library Director or designee.

9. Contracts for independent compliance/security reviews and/or testing shall indicate the types of tests to be performed, the tools to be used, and the timeframe for the tests. Contracts shall specify that the third party contractor shall not exploit vulnerabilities or perform denial of service tests unless there is a specific need that is being addressed, or is required by applicable regulations. The contractor shall not perform any such tests or scan without prior written authorization from the YVL Library Director or designee.

10. Vulnerabilities identified during compliance/security reviews shall be assessed to determine what actions may be necessary. Necessary remediation, mitigations, or risk acceptances shall be documented and approved by the YVL Library Director or designee.

11. Intrusion detection/prevention technology shall be utilized and kept current to monitor for suspicious activity entering or leaving production environment. Information concerning vulnerabilities shall be released on need-to-know basis and shall be encrypted during transmission over open networks.

14. Change Control

A. **General Policy:** It is the policy of Yakima Valley Libraries to manage change to information technology in such a way as to minimize the possibility of corruption of information systems. Strict controls over changes are required to ensure integrity of information systems is maintained.

B. **Procedure:** Standard change control practices shall include but not be limited to:

1. All changes to a production environment must follow established change control process to ensure that only authorized changes are made to production systems. Change control procedures must be followed for all significant changes to production system component's operating system, software, applications, hardware, and communications links.

2. A separate test environment should be used (when possible) to prevent negative impacts on the production environment. Systems used for development and test should be physically and/or logically segregated from production systems.

3. If possible, all changes will be first tested in a separate test environment.

4. For changes to information systems managed or operated by Yakima Valley Libraries, internal change control ticketing system shall be utilized.

5. All changes must be formally approved by authorized departmental managers, YVL Library Director, and appropriate Technology Services personnel.

6. For changes to information systems managed by a Yakima Valley Libraries authorized service provider, only designated Yakima Valley Libraries' personnel shall be authorized to request change. All change requests shall also be recorded internally for accountability purpose.

7. Change management meetings should be conducted at least every week to review scheduled change requests, assess the impacts, ensure back-out plans, determine and review potential failures, and make decisions.

8. A change management log must be maintained for all changes. This log must contain but is not limited to: date of submission, employee responsible for implementing the change, approver information, information about change itself, back-out plans, and potential impact.

15. Electronic Data Retention

A. **General Policy:** Any and all information that is created, sent, received, or stored electronically is an important Yakima Valley Libraries' asset. This policy is intended to ensure that employees determine what information should be, or is being, retained and for how long. This policy provides a framework for compliance with federal and state regulations, and applicable requirements set forth by Payment Card Industry Data Security Standard (PCI DSS) and other applicable federal, state and local standards. In addition, this policy serves to develop a consistent approach to the retention and disposal of electronic records.

B. **Procedure:**

1. This standard applies to all systems owned by Yakima Valley Libraries regardless of who manages them, that is, this standard applies to all systems managed by Yakima Valley Libraries personnel or by authorized third party service provider or contractor. Yakima Valley Libraries is responsible to communicate these retention requirements to its employees, agents, contractors, or third parties, responsible for managing or operating Yakima Valley Libraries' information systems.

2. Confidential or proprietary information when no longer needed for legal, regulatory, or business reasons shall be disposed of as defined within the Yakima Valley Libraries' records retention policy.

3. This standard does not cover operational retention that occurs through backup and/or mirroring of systems. These backups are to be used for system restoration purposes only. Yakima Valley Libraries will not attempt to recover data, files, or other information from backups or mirrors unless required to do so by law or the administration.

4. Yakima Valley Libraries will keep cardholder data storage to the minimum necessary for business purposes.

C. **Disposal:** Confidential information when no longer needed for legal, regulatory, or business reasons shall be disposed of as defined within the Library's Records Retention Policy, as now or hereinafter adopted.

D. **Retention Period:** Data shall be retained for a minimum time as specified either in the chart below, The State of Washington Local Government Common Retention Schedule located at: http://www.sos.wa.gov/archives/RecordsManagement/Records-Retention-Schedules-for-Library-Districts.aspx, or in the Library's Records Retention Policy, as now or hereinafter adopted.

DATA TYPE	MINIMUM RETENTION PERIOD
ANTIVIRUS LOGS	90 DAYS ONLINE, 12 MONTHS TOTAL
EMAIL CORRESPONDENCE	SEE STATE RETENTION SCHEDULE
EVIDENCE OF LOG REVIEWS, AUDIT LOGS	90 DAYS ONLINE, 12 MONTHS TOTAL
FINANCIAL RECORDS	SEE STATE RETENTION POLICY
HIPAA DATA	SEE STATE RETENTION POLICY
INSTANT MESSAGE	SEE STATE RETENTION SCHEDULE
PERSONNEL RECORDS	SEE STATE RETENTION POLICY
QUARANTINED SPAM	7 CALENDAR DAYS
RECORDED TELEPHONE CALLS	SEE STATE RETENTION SCHEDULE
SECURITY INCIDENT LOGS	90 DAYS ONLINE, 12 MONTHS TOTAL
SYSTEM ACCESS, USE, AND AUDIT LOGS	90 DAYS ONLINE, 12 MONTHS TOTAL
TEXT MESSAGE	SEE STATE RETENTION SCHEDULE
VIDEO CAMERA LOGS	90 DAYS
VIDEO FROM SECURITY CAMERAS	SEE STATE RETENTION SCHEDULE
VOICE MAIL	7 CALENDAR DAYS
WEBSITE	SEE STATE RETENTION SCHEDULE

16. Computing Security

A. **General Policy:** It is the policy of Yakima Valley Libraries to manage, maintain and operate a physically secure computing environment.

B. **Procedure:**

1. The IT Department shall be responsible to operate, maintain, backup and replace all library servers.

2. The IT Department shall ensure that all servers are maintained within appropriate logical and physical security zones required by their respective functions. Electronic firewalls, routers, switches, un-interruptible power supplies and physical security shall be employed as necessary to accomplish operational necessities.

3. Adequate backup and recovery practices, equipment and methods shall be maintained.

4. Backup media shall be stored off-site from the physical servers to ensure business continuity.

5. Business continuity and disaster recovery plans and practices shall be maintained and reviewed on a periodic basis.

6. Physical access to the Library computer equipment will be limited to those who have been specifically authorized by the Library Director or IT Manager

17. Application Development and Systems

A. **General Policy:** It is the policy of Yakima Valley Libraries to provide adequate information system employees to facilitate service to constituents. All systems, whether new or currently operational, will be monitored and administered by the YVL IT Department.

B. **Procedure:**

1. Whenever economically and functionally feasible commercial off the shelf software (COTS) shall be purchased for Library use.

2. If software is to be developed in-house that will be used by more than one employee, then such development shall be done under the direct oversight, review and approval by the YVL Director and YVL IT Department. Software will be documented for future support and maintenance and specific system deliverables will be listed and approved prior to project start.

3. If an individual wishes to develop an application for their own Library work related use, then they are responsible for all maintenance, upkeep, backup and troubleshooting on that application.

4. All third party software developers and vendors shall be vetted and approved by YVL IT Department who will ensure that methods, tools, design and execution will fit in and interoperate within the Library environment. Specific deliverables, milestones, acceptance criteria and operational parameters will be developed and monitored by Technology Services. Final sign off and acceptance will include the group leader who will be using the system and YVL Director or their designee.

5. All software that is developed shall be written in YVL IT Department approved languages and tools. These are to be approved prior to contract signing.

6. Software developed for or by Yakima Valley Libraries shall be the property of Yakima Valley Libraries unless expressly stated otherwise in the development contract. When stipulated in the contract, source code shall be placed in escrow by the developer and made available to Yakima Valley Libraries in the event that vendor is not able to provide adequate support.

7. It shall be standard practice to maintain an ongoing support relationship with Library vendors.

8. YVL Technology Department employees shall operate, maintain, patch and upgrade all Yakima Valley Libraries' systems. It shall be the responsibility of the user community to provide application specialists who are familiar with front end processes and able to provide training to other users and help support the back end administrators.

18. Software Licensing

A. **General Policy:** It is the policy of Yakima Valley Libraries that all general office software licensing shall be retained, monitored, supervised, and maintained by YVL IT Department. This will include but not be limited to all major business systems, desk top automation, operating systems, virus and malware software, email and other software in general use by Library employees.

B. Procedure:

1. Software that falls outside of the general use category may be purchased and licensed by departments provided it is purchased through proper channels and the original license is forwarded to YVL IT Department for inventory purposes.

2. Software that is found on machines without a proper license shall be removed immediately and until a proper license is purchased.

3. "Free downloads" of software shall be examined with the IT Manager prior to any action being taken to download or install. All free software will be logged and tracked by the IT Department.

EMPLOYEE ACKNOWLEDGEMENT OF YAKIMA VALLEY LIBRARIES POLICY ON INFORMATION TECHNOLOGY AND USE OF RESOURCES

Please read the IT Policy and Use of Resources document carefully before signing. This document clarifies policies and procedures for the Library's use of technology systems, telecommunications, Internet use, and technology management.

My signature below indicates that I have read, understand and agree to abide by Yakima Valley Libraries' Technology Policy. I understand and agree that a violation of these policies or applicable local, state, and/or federal laws may result in the immediate loss of all computer e-mail, and Internet privileges. In addition, disciplinary action may be taken against any employee who violates the policy according to the Library's Personnel Policies.

Name: ______________________ Department: ____________

Title/Position: ______________________________________

Employee Signature: ____________________ Date: __________

Supervisor Signature: ____________________ Date: __________

Please send a signed copy of this document to the IT Manager for processing. Once received employee profiles will be activated.