MVLS/SALS JOINT AUTOMATION PROJECT

Information Security Policy

Version 1.1

Approved by:

MVLS/SALS Joint Automation Council
January 11, 2017

SALS Board of Trustees
January 17, 2017

MVLS Board of Trustees
January 19, 2017

Table of Contents

Introduction

[MVLS/SALS Joint Automation Project] is hereinafter referred to as "the ORGANIZATION."

Overview

This security policy was created to communicate the requirements for secure use of ORGANIZATION resources, and represents the ORGANIZATION's strategy for how it will implement Information Security principles and technologies. This security policy differs from security processes and procedures, in that the policy provides both high level and specific guidelines on how the ORGANIZATION is to protect its data, but does not specify exactly how that is to be accomplished. This provides leeway to choose which security devices and methods are best in consideration of all factors. This policy is technology and vendor independent, as its intent is to set policy only, which can then be implemented in any manner that accomplishes the specified goals.

Scope

The security policy covers the ORGANIZATION's information systems and resources. Perhaps more importantly, it covers the ORGANIZATION data stored on these systems as well as any backups or hardcopies of this data.

Where credit card data is stored or transmitted (i.e., the cardholder data environment), more restrictive requirements will apply. Thus, the ORGANIZATION should limit the scope of the cardholder data environment to the fullest extent possible.

This policy applies to the MVLS/SALS Joint Automation Project network, which includes the Southern Adirondack Library System in Saratoga Springs, ~~as well as the WAN (staff networks at Clifton Park Halfmoon Public Library in Clifton Park, Crandall Public Library in Glens Falls, Saratoga Springs Public Library in Saratoga Springs and Schenectady County Public Library in Schenectady);~~ and to all Joint Automation staff, MVLS and SALS staff and member library staff with:

a) Physical access to the above network ~~(IT staff at Clifton Park, Crandall, Saratoga Springs and Schenectady County libraries)~~
b) Or, MVLS/SALS Joint Automation ~~Email~~ Microsoft 365 tenant or Polaris ILS access

Goals

The goals of this security policy are to accomplish the following:

1. To allow for the confidentiality and privacy of the ORGANIZATION's information.

2. To provide protection for the integrity of the ORGANIZATION's information.

3. To provide for the availability of the ORGANIZATION's information.

This is commonly referred to as the "CIA Triad" of Confidentiality, Integrity, and Availability, an approach which is shared by all major security regulations and standards. Additionally, this approach is consistent with generally-accepted industry best practices for security management.

Intent

This security policy indicates senior management's commitment to maintaining a secure network, which allows the IT Staff to do a more effective job of securing the ORGANIZATION's information assets.

A security policy may also provide legal protection to the ORGANIZATION, by specifying exactly how users can and cannot use the network, how they should treat confidential information, and the proper use of encryption.

It is the intent of this security policy to clearly communicate the requirements necessary for compliance with any applicable regulations, specifically the Payment Card Industry Data Security Standard Version 3.1 (PCI DSS 3.1), as well as any data confidentiality agreements with third parties.

Implementation

This policy requires the appointment of an Information Security Manager, who will be responsible for implementation and ongoing security administration. Specific guidance on this position can be found within this document. The Information Security Manager doesn't necessarily need to be an independent position, but can be a designation fulfilled by an existing employee (i.e., the IT Manager) as long as that employee has the authority to hold a management role, and the resources and abilities to commit to the position. This policy must be implemented with full support of management and/or the executive team.

Policies designated as "End User" policies must be distributed to and formally accepted in writing by the users. Specific guidance regarding security policy implementation and ongoing management can be found within this document.

Revision History

Revision	Date	Notes
Revision 1.0	5/31/2016	First Revision

I. Acceptable Use Policy

[MVLS/SALS JOINT AUTOMATION PROJECT] is hereinafter referred to as "the ORGANIZATION."

1.0 Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using ORGANIZATION resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

2.0 Purpose

Since inappropriate use of corporate systems exposes the ORGANIZATION to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

3.0 Scope

The scope of this policy includes any and all use of corporate information resources, including but not limited to, computer systems, email, the network, and the corporate internet connection.

4.0 Policies

4.1 Web Browsing and Internet Usage

The internet is a network of interconnected computers of which the ORGANIZATION has very little control. The user must recognize this when using the internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate, or that may be illegal in some jurisdictions. The user must use the internet at his or her own risk. The ORGANIZATION is

specifically not responsible for any information that the user views, reads, or downloads from the internet.

4.1.1. Personal Use

The ORGANIZATION recognizes that the internet can be a tool that is useful for both personal and professional purposes. Personal usage of ORGANIZATION computer systems to access the internet is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the ORGANIZATION or on the user's job performance.

4.1.2 Peer-to-Peer File Sharing

Peer-to-Peer (P2P) file sharing/networking is not allowed on the corporate network under any circumstance. P2P is a distributed network of users who share files by directly connecting to the users' computers over the internet rather than through a central server.

4.1.3 Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Reasonable use of streaming media is permitted as long as it does not negatively impact the computer network or the user's job performance.

4.1.4 Instant Messaging

The user should recognize that instant messaging technology, unless specific encryption measures are taken, is an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data. Unencrypted confidential data must never be sent via instant messaging technologies. Primary Account Numbers (PANs) must never be sent via instant messaging, regardless of encryption.

4.1.5 Bandwidth Usage

Excessive use of ORGANIZATION bandwidth or other computer resources, where not required by job function, is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low ORGANIZATION-wide usage. The ORGANIZATION may restrict bandwidth for certain services

deemed non-critical to ORGANIZATION operations, or as it sees fit to preserve network functionality.

4.1.6 Social Networking/Social Media/Blogs/Websites

Social networking and posting to blogs or websites is subject to the terms of this policy, whether performed from the ORGANIZATION network, personal systems, or other external systems. Use of these sites creates risks for the ORGANIZATION in two ways: 1) in the potential sharing of ORGANIZATION confidential, private, or embarrassing information, and 2) the potential for an attacker to use posted information to craft a social engineering attack on the ORGANIZATION. The user is asked to recognize that information posted on social networking sites, blogs or websites is public information and to exercise extreme discretion in the type of information posted. No confidential information or other sensitive information of the ORGANIZATION are to be posted on social networking sites, blogs or websites. Further, the user should restrict his or her privacy settings to fullest extent possible. The user must not publish any information detrimental to the ORGANIZATION, or that would cause embarrassment to the ORGANIZATION, on social networking sites.

As long as ORGANIZATION policies, as specified herein, are followed, the ORGANIZATION allows reasonable use of social networking sites from its network. This use must be business related and consume no more than a trivial amount of network resources. The user assumes all risks associated with social networking.

4.2 Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network. This section is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable.

4.2.1 Prohibited Actions

The user may not use the corporate network and/or systems to:

- Reveal personal or network usernames or passwords to others, including family, friends, or other members of the household when working from home or remote locations.
- Engage in activities that cause an invasion of privacy.

- Engage in activity that is illegal under local, state, federal, or international law (see section "Use for Illegal Activities" for more information).

- Engage in any action prohibited in the local library policy or employee handbook.

4.2.2 Circumvention of Security

Using ORGANIZATION-owned ORGANIZATION-provided, or personal computer systems to circumvent any security systems, authentication systems, user-based systems, or the escalation of privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent ORGANIZATION security systems is expressly prohibited. This includes disabling or tampering with any ORGANIZATION supplied security software, such as antivirus/anti-malware software or remote access software.

4.2.3 Use for Illegal Activities

No ORGANIZATION-owned or ORGANIZATION-provided computer systems may be used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning.

- Unauthorized Network Hacking, including: packet sniffing, port scanning, packet spoofing, denial of service, wireless hacking.

- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system.

- Acts of Terrorism.

- Cybercrime, extortion, or Identity Theft.

- Downloading, storing, or distributing any material prohibited by law.

- Downloading, installing, or distributing unlicensed or "pirated" software.

- Sending unsolicited bulk email or other messages deemed illegal under applicable regulations.

The ORGANIZATION will take all necessary steps to report and prosecute any violations of this policy.

4.2.4 Copyright Infringement

The ORGANIZATION's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of the Acceptable Use Policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed storage media; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

4.3 Monitoring and Privacy

Users should expect no privacy when using the corporate network or ORGANIZATION resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The ORGANIZATION reserves the right to monitor any and all use of the computer network. To ensure compliance with ORGANIZATION policies this may include the interception and review of any emails, or other messages sent or received; inspection of data stored on personal file directories, hard disks, and removable media; and monitoring of internet/network usage.

4.4 Responsible Computer and Network Use

The ORGANIZATION expects users to use the network responsibly. Personal usage of ORGANIZATION computer systems is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the ORGANIZATION or on the user's job performance.

4.4.1 Non-ORGANIZATION-Owned Equipment

Non-ORGANIZATION-provided computer equipment is expressly prohibited from being connected to the ORGANIZATION's network. Examples of this are: laptops, notebooks, tablet computers, smartphones, etc. These devices may be connected to the “public” wireless network.

4.4.2 Removable Media

Personal (non-ORGANIZATION-owned) storage devices can represent a serious threat to data security when connected to the ORGANIZATION's network. Examples of this are: USB drives, flash storage, media players, etc. All computers should be properly protected with antivirus software and that software should not be tampered with in order to use removable media that otherwise would not pass configured security scans.

Storage media supplied by the ORGANIZATION is allowed, however guidelines on confidential/cardholder data, such as those found in the Confidential Data and Mobile Device Policies, must be strictly followed.

4.4.3 Software Installation

Installation of non-ORGANIZATION-supplied software applications is prohibited, without prior permission from the Information Security Manager. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.

4.5 Reporting of a Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.)
- Suspected virus/malware/Trojan infection
- Loss or theft of any device that contains ORGANIZATION information
- Loss or theft of ID badge, keycard, or two-factor authentication token
- Any attempt by any person to obtain a user's password over the telephone or by email
- Any other suspicious event that may impact the ORGANIZATION's information security

Users must treat a suspected security incident as confidential information, and report the incident only to their supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

4.6 Applicability of Other Policies

This document is part of the ORGANIZATION's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

This policy will be enforced by the MVLS/SALS Joint Automation Information Security Manager and/or Executive Team. Violations will be reported to the member public library director and may result in suspension or restriction of access to all MVLS/SALS services. Where illegal activities or theft of ORGANIZATION property (physical or intellectual) are suspected, the ORGANIZATION may report such activities to the applicable authorities.

II. Password Policy

[MVLS/SALS Joint Automation Project] is hereinafter referred to as "the ORGANIZATION."

1.0 Overview

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

2.0 Purpose

The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

3.0 Scope

This policy applies to every person who is provided an account on the ORGANIZATION's network or systems, including: employees, guests, contractors, partners, vendors, etc.

4.0 Policies

4.1 Construction

The best security against a password incident is simple: following a sound password construction strategy. The ORGANIZATION mandates that users adhere to the following guidelines on password construction:

- Passwords must be at least 8 characters.
- Passwords must be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols). Specifically, they must contain characters from 3 of the following 4 categories: uppercase, lowercase, digits 0 – 9, and non-alphabetic characters
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)

- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this was as well: an 'S' can become a '$' or an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

4.2 Confidentiality

Passwords are considered confidential data and treated with the same discretion as any of the ORGANIZATION's proprietary information. The following guidelines apply to the confidentiality of ORGANIZATION passwords:

- Users must not disclose their passwords to anyone, including other staff or MVLS/SALS Joint Automation staff.
- Users must not share their passwords with others (co-workers, supervisors, family, etc.).
- Users must not write down their passwords and leave them unsecured.
- Users must not check the "save password" box when authenticating to applications, especially on mobile devices or shared devices.
- Users must not use the same password for different systems and/or accounts.
- Users must not send passwords via email.
- Users must not re-use passwords.
- User must not allow others to use their accounts.
- Staff must never allow patrons to use staff accounts on any PC.

4.3 Change Frequency

In order to maintain good security, passwords must be periodically changed. This limits the damage an attacker can do as well as helps to frustrate and slow attempts to crack a password through brute force. At a minimum, the ORGANIZATION must require users to change their

passwords every 180 days (or more frequently at the discretion of the Information Security Manager). IT staff are required to change passwords every 90 days. The ORGANIZATION may use software that enforces this policy by expiring users' passwords after this time period. When selecting a new password, users must not select a password that is substantially the same as, or similar to, any of the previous four passwords used.

4.4 Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving their passwords to the Information Security Manager and immediately change the password in question. Staff should never respond to a request to reveal their password to anyone, including other staff personnel. When a password is suspected to have been compromised the Information Security Manager will request that the user, or users, change all their passwords.

4.5 Applicability of Other Policies

This document is part of the ORGANIZATION's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

This policy will be enforced by the MVLS/SALS Joint Automation Information Security Manager and/or Executive Team. Violations will be reported to the member public library director and may result in suspension or restriction of access to all MVLS/SALS services. Where illegal activities or theft of ORGANIZATION property (physical or intellectual) are suspected, the ORGANIZATION may report such activities to the applicable authorities.

III. Email Policy

[MVLS/SALS Joint Automation Project] is hereinafter referred to as "the ORGANIZATION."

1.0 Overview

Email is an essential component of business communication; however it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email can also have an effect on the ORGANIZATION's liability by providing a written record of communications, so having a well thought out policy is essential. This policy outlines expectations for appropriate, safe, and effective email use.

2.0 Purpose

The purpose of this policy is to detail the ORGANIZATION's usage guidelines for the email system. This policy will help the ORGANIZATION reduce risk of an email-related security incident, foster good business communications both internal and external to the ORGANIZATION, and provide for consistent and professional application of the ORGANIZATION's email principles.

3.0 Scope

The scope of this policy includes the MVLS/SALS Joint Automation email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the ORGANIZATION network.

4.0 Policies

4.1 Proper Use of ORGANIZATION Email Systems

Users are asked to exercise common sense when sending or receiving email from ORGANIZATION accounts. Additionally, the following applies to the proper use of the ORGANIZATION email system.

4.1.1 Sending Email

When using an ORGANIZATION email account, email must be addressed and sent carefully. Users should keep in mind that the ORGANIZATION loses any control of email once it is sent external to the ORGANIZATION network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help the ORGANIZATION avoid the unintentional disclosure of sensitive or non-public information.

4.1.2 Personal Use

Personal usage of ORGANIZATION email systems is permitted as long as A) such usage does not negatively impact the corporate computer network, and B) such usage does not negatively impact the user's job performance. Users should expect no privacy when using the corporate network or ORGANIZATION resources.

4.1.3 Business Communications and Email

The ORGANIZATION uses email as an important communication medium for business operations. Users of the corporate email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, users are asked to recognize that email sent from an ORGANIZATION account reflects on the ORGANIZATION, and, as such, email must be used with professionalism and courtesy.

4.1.4 Email Signature

An email signature (contact information appended to the bottom of each outgoing email) is recommended for all emails sent from the ORGANIZATION email system. At a minimum the signature should include the user's:

- Title
- ORGANIZATION name
- Phone number(s)
- Fax number, if applicable

Email signatures should not include personal messages (political, humorous, etc.). The IT Staff is able to assist in email signature setup if necessary.

4.1.5 Out-of-Office Reply

The ORGANIZATION recommends the use of an out-of-office reply (if the email system is equipped with such a feature) if the user will be out of the office for an extended period of time. The reply must notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required.

4.1.6 Mass Emailing

The ORGANIZATION makes the distinction between the sending of mass emails and the sending of unsolicited bulk email (spam). Mass emails may be useful for library notification and promotions, and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

It is the ORGANIZATION's intention to comply with applicable laws governing the sending of mass emails. For this reason, as well as in order to be consistent with good business practices, the ORGANIZATION requires that email sent to more than twenty-five (25) recipients external to the ORGANIZATION have the following characteristics:

- The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honored immediately.

- The email must be addressed to all recipients using the BCC (blind carbon copy) option, so that each recipient only sees their own address.

- The email must contain a subject line relevant to the content.

- The email must contain contact information, including the full physical address, of the sender.

- The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.

4.1.7 Opening Attachments

Users must use extreme care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users must:

- Never open unexpected email attachments.
- Never open email attachments from unknown sources.
- Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially-formatted emails can hide a malicious URL.

The ORGANIZATION may use methods to block what it considers to be dangerous emails or strip potentially harmful email attachments as it deems necessary.

4.1.8 Monitoring and Privacy

Users should expect no privacy when using the corporate network or ORGANIZATION resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The ORGANIZATION reserves the right to monitor any and all use of the computer network. To ensure compliance with ORGANIZATION policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.1.9 ORGANIZATION Ownership of Email

Users should be advised that the ORGANIZATION owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the ORGANIZATION and it may be subject to use for purposes not anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.

4.1.10 Contents of Received Emails

Users must understand that the ORGANIZATION has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, the ORGANIZATION may attempt to reduce the amount of this email that the users receive, however no solution will be 100% effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she must notify his or her supervisor.

4.1.11 Access to Email from Mobile Devices

Many mobile devices provide the capability to send and receive email. This can present a number of security issues, particularly relating to the storage of email, which may contain sensitive data, on the device. ~~Users are only allowed to access the MVLS/SALS Joint Automation email system from mobile devices via the web-based interface or app, which does not store email on the device.~~ Users of the MVLS/SALS Joint Automation email system are only allowed to use the encrypted web-based interface, installed Outlook on a PC, or Outlook app on portable devices

~~Users must never save passwords for email on any mobile device.~~ Users must use a device password or authentication to lock/unlock the device. Mobile device OS and apps must be on current and supported versions.

4.2 Confidential Data and Email

The following sections relate to confidential data and email:

4.2.1 Passwords

As with any ORGANIZATION passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the Information Security Manager, the ORGANIZATION may further secure email with certificates, two-factor authentication, or another security mechanism.

4.2.2 Emailing Confidential or Sensitive Data

Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

The ORGANIZATION requires that any email containing confidential information, regardless of whether the recipient is internal or external to the ORGANIZATION network, be encrypted using strong encryption.

Further guidance on the treatment of confidential information exists in the ORGANIZATION's Confidential Data Policy. If information contained in the Confidential Data Policy conflicts with this policy, the Confidential Data Policy will apply.

Guidance on the treatment of sensitive information exists in ~~JA's Sensitive Data Policy~~ the Confidential Library Patron Data and Confidential Personnel and Financial Data policies.

4.2.3 Emailing Cardholder Data for credit/debit cards

The ORGANIZATION must ensure Primary Account Numbers (PANs) are never sent via end-user messaging technologies, regardless of encryption used. End user messaging technologies include email, instant-messaging, and any other digital communication meant for end-users. A product that provides data loss prevention functions may be useful for this requirement.

4.3 ORGANIZATION Administration of Email

The ORGANIZATION will use its best effort to administer the ORGANIZATION's email system in a manner that allows the user to both be productive as well as reduce the risk of an email-related security incident.

4.3.1 Filtering of Email

A strategy to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, the ORGANIZATION may choose to filter email at the internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed A) contrary to this policy, or B) a potential risk to the ORGANIZATION's IT security. No method of email filtering is 100% effective, so the user is asked additionally to be cognizant of this policy, manage filtered emails responsibly and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of the Information Security Manager.

4.3.2 Email Disclaimers

The use of an email disclaimer, usually text appended to the end of every outgoing email message, is an important component in the ORGANIZATION's risk reduction efforts. The ORGANIZATION requires the use of email disclaimers on every outgoing email, which must contain the following notices:

- The email is for the intended recipient only.
- The email may contain private information.
- If the email is received in error, the sender must be notified and any copies of the email destroyed.
- Any unauthorized review, use, or disclosure of the contents is prohibited.

A disclaimer similar to the following is automatically appended to all outgoing MVLS/SALS Joint Automation email:

If you believe you have received this message in error or do not wish to receive this information via email, please reply to this message. This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this email. To report this message as spam or offensive, please send e-mail to abuse@sals.edu including the entire contents and subject of the message.
It will be reviewed by staff and acted upon appropriately.

The ORGANIZATION must review any applicable regulations relating to its electronic communication to ensure that its email disclaimer includes all required information.

4.3.3 Email Deletion

Users are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable, and reduce the burden on the ORGANIZATION to store and backup unnecessary email messages.

Please note that users are strictly forbidden from deleting email in an attempt to hide a violation of this or another ORGANIZATION policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

4.3.4 Retention and Backup

Email must be retained and backed up in accordance with the applicable policies, which may include but are not limited to the: ~~Sensitive~~ Confidential Library Paton Data Policy, Confidential Personnel and Financial Data Policy~~, Backup Policy, and Retention Policy~~ and Security Description addendum.

4.3.5 Account Activation

Email accounts will be set up for each user determined to have a business need to send and receive ORGANIZATION email. Accounts will be set up at the time a new hire starts with the ORGANIZATION, or when a promotion or change in work responsibilities for an existing employee creates the need for email access.

Accounts on the MVLS/SALS Joint Automation email system will never be provided to non-employees of the MVLS/SALS member libraries that JA serves, such as contractors, vendors or library trustees.

4.3.6 Account Termination

When a user leaves employment at an MVLS/SALS member library, JA should be notified immediately so that JA can disable the user's access to the account by password change, disabling the account, or another method. Please note that JA is under no obligation to block the account from receiving email, and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by the MVLS/SALS member library.

4.3.7 Storage Limits

As part of the email service, email storage may be provided on ORGANIZATION servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the Information Security Manager. Storage limits may vary by employee or position within the ORGANIZATION.

4.4 Prohibited Actions

The following actions shall constitute unacceptable use of the corporate email system. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate email system to:

- Send any information that is illegal under applicable laws.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the ORGANIZATION may not be sent via email, regardless of the recipient, without proper encryption.
- Send Credit Card Primary Account Numbers (PANs) via email, regardless of encryption.
- Attempt to impersonate another person or forge an email header.
- Send spam, solicitations, chain letters, or pyramid schemes.
- Knowingly misrepresent the ORGANIZATION's policies.

The ORGANIZATION may take steps to report and prosecute violations of this policy, in accordance with ORGANIZATION standards and applicable laws.

4.4.1 Data Leakage

Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to the ORGANIZATION's control of its data.

Unauthorized emailing of ORGANIZATION data, confidential or otherwise, to external email accounts for the purpose of saving this data external to ORGANIZATION systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user must notify their supervisor rather than emailing the data to a personal account or otherwise removing it from ORGANIZATION systems.

Automatic blind forwarding of email to an external email address is prohibited.

The ORGANIZATION may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the Information Security Manager.

4.4.2 Sending Large Emails

Email systems were not designed to transfer large files and as such emails must not contain attachments of excessive file size. The ORGANIZATION asks that the user limit email attachments to a reasonable size.

The user is further asked to recognize the additive effect of large email attachments when sent to multiple recipients, and use restraint when sending large files to more than one person.

4.5 Applicability of Other Policies

This document is part of the ORGANIZATION's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

This policy will be enforced by the MVLS/SALS Joint Automation Information Security Manager and/or Executive Team. Violations will be reported to the member public library director and may result in suspension or restriction of access to all MVLS/SALS services. Where illegal activities or theft of ORGANIZATION property (physical or intellectual) are suspected, the ORGANIZATION may report such activities to the applicable authorities.

IV. Remote Access Policy

[MVLS/SALS Joint Automation Project] is hereinafter referred to as "the ORGANIZATION."

1.0 Overview

It is often necessary to provide access to corporate information resources to employees or others working outside the ORGANIZATION's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation. This Remote Access Policy does not relate to regular MVLS/SALS services such as the ILS or email. This policy refers to users of the VPN (Virtual Private Network software) such as Joint Automation, member library IT and system staff.

2.0 Purpose

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

3.0 Scope

The scope of this policy covers all employees, contractors, and external parties that access ORGANIZATION resources over a third-party network, whether such access is performed with ORGANIZATION-provided or non-ORGANIZATION-provided equipment. Joint Automation staff, MVLS system staff and SALS system staff are only allowed to use ORGANIZATION-provided equipment for VPN access. Library IT staff are permitted to use non-ORGANIZATION-provided equipment and VPN (configured with ~~host scan~~ security scanning and limited access).

4.0 Policies

4.1 Remote Access Client Software

The ORGANIZATION will supply users with remote access software that allows for secure access when outside the network and enforces the remote access policy. The software will provide strong traffic encryption in order to protect the data during transmission.

For the purpose of this policy, ownership of the remote device is irrelevant. If the device ever connects to the ORGANIZATION network this policy applies to that device.

4.2 Remote Network Access

Remote network access can be provided for a variety of reasons to a variety of different types of users. Rather than take a "one size fits all" approach, the ORGANIZATION requires that remote access be offered according to the level of access required by each user type, as specified below.

4.2.1 Employees

Due to the elevated risk of remote access, two-factor authentication (such as smart cards, tokens, or biometrics in combination with a password) must be used. The ORGANIZATION will limit remote users' access privileges to only those information assets that are reasonable and necessary to perform their job function when working remotely (i.e., email). The entire network must not be exposed to remote access connections.

4.2.2 Administrators

Due to the elevated risk of remote access, two-factor authentication (such as smart cards, tokens, or biometrics in combination with a password) must be used. Any non-console administrative access, such as remote management or web-based access, must be secured to prevent misuse. If such access is allowed, it must meet the following criteria:

- Remote administrative access must be encrypted using strong encryption that is initiated prior to the administrative password being requested.

- Insecure management protocols, such as telnet, must be disabled or prohibited in favor of more secure methods, such as SSH, or encrypted via a VPN or SSL/TLS.

4.2.3 Third Parties/Vendors

Due to the elevated risk of remote access, two-factor authentication (such as smart cards, tokens, or biometrics in combination with a password) must be used. When non-employees are provided access to the network, such as vendors or service providers, their remote access account must

be disabled when not in use. Further, accounts used for remote vendor access must be monitored when in use.

~~4.3 Idle Connections~~

~~Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the ORGANIZATION's network must be timed out after 15 minutes of inactivity.~~

4.4 Prohibited Actions

Remote access to corporate systems is only to be offered through an ORGANIZATION-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on an ORGANIZATION system without the approval of the Information Security Manager.
- Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the Information Security Manager.
- Use of non-ORGANIZATION-provided remote access software.
- On non-ORGANIZATION-provided devices, split Tunneling to connect to an insecure network in addition to the corporate network, or in order to bypass security restrictions.
- Copying data to, and storing data on, remote computers unless explicitly authorized to do so for a defined business need and done in a manner that meets requirements for data confidentiality. If the data contains cardholder data, the ORGANIZATION must comply with any applicable PCI Data Security Standard requirements as well.

4.5 Use of non-ORGANIZATION-provided Systems

Accessing the corporate network through home or public systems presents a security risk, as the ORGANIZATION cannot completely control the security of the system accessing the network. No non-ORGANIZATION-provided computers are allowed to access the corporate network for any reason, unless the access is provided by the ORGANIZATION in a public manner, such as web-

based email. Member library IT staff and contract employees are permitted limited access from their own devices. Such access will require VPN with ~~hostscan~~ security scanning and be limited to only that member library's network and/or servers.

4.6 Applicability of Other Policies

This document is part of the ORGANIZATION's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

This policy will be enforced by the MVLS/SALS Joint Automation Information Security Manager and/or Executive Team. Violations will be reported to the member public library director and may result in suspension or restriction of access to all MVLS/SALS services. Where illegal activities or theft of ORGANIZATION property (physical or intellectual) are suspected, the ORGANIZATION may report such activities to the applicable authorities.

V. Confidential Library Patron Data Policy

[MVLS/SALS Joint Automation Project] is hereinafter referred to as "the ORGANIZATION."

1.0 Overview

For this document, we have defined two classifications for data that requires additional security policies and procedures:

- Confidential Library Patron data:
  - Addresses, phone numbers, email addresses, driver's license numbers, reading history for staff and/or ILS patrons
- Confidential Personnel and Financial data:
  - Payroll, banking, social security numbers for JA and system staff; member libraries should have a similar local policy in place for this data
  - Credit Card data – all data pertaining to credit cards; for MVLS/SALS Joint Automation no credit card data is retained on JA servers or the ILS, ~~however it does pass through the MVLS/SALS Joint Automation network (in an encrypted format) when credit card payments are accepted on pin/pad terminals connected to self-checks and/or staff workstations.~~ For accepting credit card payments via the PAC, credit card data is never on our network or servers because the payment is made from outside our network and it is done via https (redirect and postback method) directly to a 3rd party.

This section addresses Confidential Library Patron Data.

2.0 Purpose

The purpose of this policy is to detail how to identify and handle confidential library patron data. This policy lays out standards for the classification and use of confidential library patron data, and outlines specific security controls to protect this data.

3.0 Scope

The scope of this policy covers all ORGANIZATION confidential library patron data, regardless of location. Also covered by the policy are hardcopies of ORGANIZATION data, such as printouts, faxes, notes, etc.

4.0 Policies

4.1 Data Classification

In order to determine how it should be handled, data must be classified according to its importance to ORGANIZATION operations and the confidentiality of its contents. Once this has been determined, the ORGANIZATION can take steps to ensure that data is treated appropriately.

Confidential library patron data must be identified and inventoried in all its forms – electronic, printed, or stored on digital media – and segregated from the ORGANIZATION's non-confidential data so that access to it can be more tightly controlled and tracked.

New York State laws regarding patron records and privacy must be followed at all times - see New York State Civil Practice Laws and Rules, Section 4509, quoted below:

> "Library records, which contain names or other personally identifying details regarding the users of public, free association, school, college and university libraries and library systems of this state, including but not limited to records related to the circulation of library materials, computer database searches, interlibrary loan transactions, reference queries, requests for photocopies of library materials, title reserve requests, or the use of audio-visual materials, films or records, shall be confidential and shall not be disclosed except that such records may be disclosed to the extent necessary for the proper operation of such library and shall be disclosed upon request or consent of the users or pursuant to subpoena, court order or where otherwise required by statute. "

4.2 Treatment of Confidential Library Patron Data

The following sections detail ORGANIZATION requirements on the storage, transmission, and destruction of data:

4.2.1 Storage

Confidential library patron data must be removed from desks, computer screens, and common areas unless it is currently in use.

Confidential library patron data must be stored in encrypted form, using strong encryption, whenever possible, when storage of this data is necessary. ~~on a mobile device, which is more~~

~~prone to theft or loss~~. Any exception must be documented and approved by the MVLS/SALS Joint Automation Information Security Manager.

Confidential library patron data must be stored only when absolutely necessary.

Confidential library patron data must never be stored on non-JA-~~provided~~approved systems (i.e., home computers, personal iPads, cell phones, non-JA cloud storage or email).

4.2.2 Transmission

Strong encryption must be used when transmitting confidential library patron data when such transmission takes place outside the ORGANIZATION's network. For example, patron authentication for databases or other electronic resources must be encrypted. Confidential library patron data must not be left on voicemail systems, either inside or outside the ORGANIZATION's network, or otherwise recorded.

Additional requirements that apply to the transmission of confidential library patron data are that the ORGANIZATION must:

- If the transmission occurs as part of a web application, ensure that HTTPS is displayed in the browser URL bar whenever confidential library patron information is requested.

4.2.3 Destruction

Media containing confidential library patron data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross-cut shredding or incineration is required in order to make the data unrecoverable.

- Storage media (CD's, DVD's): physical destruction is required, via any means that makes the data unrecoverable.

- Hard Drives/Systems/Mobile Storage Media: physical destruction is required. If physical destruction is not possible, the Information Security Manager must be notified, and the strongest commercially available data wiping technology used to ensure this data is unrecoverable.

Rather than putting the responsibility for data destruction on users, the ORGANIZATION may implement a system to ensure that data is destroyed in a manner consistent with this policy. Media awaiting destruction under this policy must be physically secured until the necessary destruction can take place. This can be in the form of a locked cabinet or other secure storage.

4.3 Examples of Confidential Library Patron Data

The following list is not intended to be exhaustive, but should provide the ORGANIZATION with guidelines on what type of information is typically considered confidential library patron. Confidential library patron data can include:

- Employee or patron personal information, such as address, email address, phone numbers
- Patron information on the ILS, such as items out, fines, reading history

4.4 Use of Confidential Library Patron Data

A successful confidential library patron data policy is dependent on the users knowing and adhering to the ORGANIZATION's standards involving the treatment of confidential library patron data. The following applies to how users must interact with confidential library patron data:

- Users must only access confidential library patron data to perform their job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential library patron information.
- Users must protect any confidential library patron information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do their job or the action is approved by their supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential library patron information immediately to their supervisor.

4.5 Sharing Confidential Library Patron Data with Third Parties

If confidential library patron data is shared with third parties, such as service providers, a written agreement must govern the provider's use of the confidential library patron information. The agreement must include the following: 1) an acknowledgement that the provider is responsible for the security of the data that it possesses, and that it will appropriately secure any data that it stores or transmits on behalf of the ORGANIZATION; and 2) how the data is to be used, transmitted, stored, destroyed.

When the ORGANIZATION will be sharing confidential library patron data with a service provider or other third party, due diligence must always be performed prior to a provider being selected. ~~Further details about due diligence can be found in the Outsourcing Policy.~~

If media containing confidential library patron data is sent external to the ORGANIZATION, rigorous security procedures must be developed and maintained, which will include, at minimum, credential-verification and signature of the service courier. Media must be sent via a delivery method that allows the media to be tracked.

4.6 Security Controls for Confidential Library Patron Data

Confidential library patron data requires additional security controls in order to ensure its integrity. The ORGANIZATION requires that the following guidelines are followed:

- Strong Encryption: Strong encryption must be used for confidential library patron data transmitted external to the ORGANIZATION.

- Physical Security: Systems that contain confidential library patron data, as well as confidential library patron data in hardcopy form, must be stored in secured areas.

- Printing: When printing confidential library patron data the user must use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential library patron data must be located in secured areas.

- Faxing: When faxing confidential library patron data, users must use cover sheets that inform the recipient that the information is confidential. Faxes must be set to print a confirmation page after a fax is sent; and the user must attach this page to the confidential library patron data if it is to be stored. Fax machines that are regularly used

for sending and/or receiving confidential library patron data must be located in secured areas.

- Emailing: Confidential library patron data must not be emailed inside or outside the ORGANIZATION without the use of strong encryption. More information can be found in the Email Policy. In the case of notification and receipts containing a patron's own data, encryption is not required as they are opting to receive this information via email. When emailing part of library patron's information without identifying the patron specifically (for example, just a barcode or just an address) that information can be transmitted without encryption.

- Mailing: If confidential library patron information is sent outside the ORGANIZATION, the user must use a service that requires a signature for receipt of that information. When sent inside the ORGANIZATION, confidential library patron data must be transported in sealed security envelopes marked "confidential." In the case of notification and receipts containing a patron's own data, signature and security envelope is not required as they are opting to receive this information via mail.

- Wireless Access: When confidential library patron data is transmitted or accessed via wireless networks, the ORGANIZATION must use wireless industry best practices for encryption, such as IEEE 802.11i. Only the strongest encryption algorithms must be used to secure this data during transmission. Please note that the use of known insecure encryption methods, such as WEP, is expressly prohibited.

- Discussion: When confidential library patron information is discussed it must be done in non-public places, and where the discussion cannot be overheard.

- Display: If confidential library patron data is written on a whiteboard or other physical presentation tool, the data must be erased immediately after the meeting is concluded.

- Media: Any media containing confidential library patron information must be physically secured in an access-controlled area. The ORGANIZATION must control all aspects of storage and accessibility of media, including storing media in secured areas.

4.7 Applicability of Other Policies

This document is part of the ORGANIZATION's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

This policy will be enforced by the MVLS/SALS Joint Automation Information Security Manager and/or Executive Team. Violations will be reported to the member public library director and may result in suspension or restriction of access to all MVLS/SALS services. Where illegal activities or theft of ORGANIZATION property (physical or intellectual) are suspected, the ORGANIZATION may report such activities to the applicable authorities.

VI. Confidential Personnel and Financial Data Policy

[MVLS/SALS Joint Automation Project] is hereinafter referred to as "the ORGANIZATION."

1.0 Overview

For this document, we have defined two classifications for data that requires additional security policies and procedures:

- Confidential Library Patron data:
  - Addresses, phone numbers, email addresses, driver's license numbers, reading history for staff and/or ILS patrons
- Confidential Personnel and Financial data:
  - Payroll, banking, social security numbers for JA and system staff; member libraries should have a similar local policy in place for this data
  - Credit Card data – all data pertaining to credit cards; for MVLS/SALS Joint Automation no credit card data is retained on JA servers or the ILS, ~~however it does pass through the MVLS/SALS Joint Automation network (in an encrypted format) when credit card payments are accepted on pin/pad terminals connected to self-checks and/or staff workstations.~~ For accepting credit card payments via the PAC, credit card data is never on our network or servers because the payment is made from outside our network and it is done via https (redirect and postback method) directly to a 3rd party.

This section addresses Confidential Personnel and Financial Data.

2.0 Purpose

The purpose of this policy is to detail how to identify and handle confidential personnel and financial data. This policy lays out standards for the classification and use of confidential personnel and financial data, and outlines specific security controls to protect this data.

3.0 Scope

The scope of this policy covers all ORGANIZATION confidential personnel and financial data, regardless of location. Also covered by the policy are hardcopies of ORGANIZATION data, such as printouts, faxes, notes, etc.

4.0 Policies

4.1 Data Classification

In order to determine how it should be handled, data must be classified according to its importance to ORGANIZATION operations and the confidentiality of its contents. Once this has been determined, the ORGANIZATION can take steps to ensure that data is treated appropriately.

Of particular concern is confidential personnel and financial data or cardholder data. This must be identified and inventoried in all its forms – electronic, printed, or stored on digital media – and segregated from the ORGANIZATION's non-confidential data so that access to it can be more tightly controlled and tracked. Any media that contains cardholder data must be catalogued and secured.

4.2 Treatment of Confidential Personnel and Financial Data

The following sections detail ORGANIZATION requirements on the storage, transmission, and destruction of confidential personnel and financial data:

4.2.1 Storage

Confidential personnel and financial data, such as cardholder data, must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential personnel and financial information must be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

Confidential personnel and financial data must be stored in encrypted form, using strong encryption, when storage of this data is necessary. Note that this requirement applies to backups containing confidential personnel and financial data as well.

Confidential personnel and financial data must be stored only when absolutely necessary. When handling cardholder data, the following must never be stored: the full contents of any track from a credit card magnetic stripe, the card verification code, and the personal identification number (PIN) or encrypted PIN block. The following data can be retained if there is a business need to do so and they are appropriately secured:

- Cardholder name

- Primary Account Number (PAN)
- Expiration Date
- Service Code

When credit card Primary Account Numbers (PANs) need to be stored, no matter what the storage medium, they must be stored in such a way that they are rendered unreadable. The most commonly used way to accomplish this is via strong cryptography and one-way hashes based on strong cryptography; however other methods can be used as well, such as index tokens and pads. No matter what method is used, the ORGANIZATION must implement guidelines for secure storage of encryption materials as well as secure processes for their use.

When credit card authentication data is received, the data must be securely deleted following authorization, using the guidelines in section 4.2.3. Processes must be implemented to ensure that this data is unrecoverable upon completion of the authorization process.

Confidential personnel and financial data must never be stored on non-ORGANIZATION-provided systems (i.e., home computers).

4.2.2 Transmission

Strong encryption must be used when transmitting confidential personnel and financial data, such as credit card data, when such transmission takes place outside the ORGANIZATION's network. Confidential personnel and financial data must not be left on voicemail systems, either inside or outside the ORGANIZATION's network, or otherwise recorded.

Additional requirements that apply to the transmission of confidential personnel and financial data are that the ORGANIZATION must:

- Only accept trusted keys and certificates. Ensure that processes are in place to verify that only trusted keys and certificates are accepted.

- Require the use of strong encryption by disabling support for weaker encryption schemes, and those with known weaknesses and/or vulnerabilities.

- Ensure that proper encryption strength is implemented for the encryption methodology in use per vendor specifications.

- If the transmission occurs as part of a web application, ensure that HTTPS is displayed in the browser URL bar whenever confidential personnel and financial information, such as cardholder data, is requested.

4.2.3 Destruction

Media containing confidential personnel and financial data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross-cut shredding or incineration is required in order to make the data unrecoverable.

- Storage media (CD's, DVD's): physical destruction is required, via any means that makes the data unrecoverable.

- Hard Drives/Systems/Mobile Storage Media: physical destruction is required. If physical destruction is not possible, the Information Security Manager must be notified, and the strongest commercially available data wiping technology used to ensure this data is unrecoverable.

Rather than putting the responsibility for data destruction on users, the ORGANIZATION may implement a system to ensure that data is destroyed in a manner consistent with this policy. Media awaiting destruction under this policy must be physically secured until the necessary destruction can take place. This can be in the form of a locked cabinet or other secure storage solution.

4.3 Examples of Confidential Personnel and Financial Data

The following list is not intended to be exhaustive, but should provide the ORGANIZATION with guidelines on what type of information is typically considered confidential personnel and financial. Confidential personnel and financial data can include:

- Credit card information/cardholder data
- Employee or customer social security numbers, or other personal information
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)

- ORGANIZATION financial data which has not been released publicly
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Any confidential personnel and financial data held for a third party (be sure to adhere to any confidential personnel and financial data agreement covering such information) and append that agreement, or a summary thereof, to this policy. Refer to section 4.6 of the Confidential Personnel and Financial Data Policy for additional information.

4.4 Use of Confidential Personnel and Financial Data

A successful confidential personnel and financial data policy is dependent on the users knowing and adhering to the ORGANIZATION's standards involving the treatment of confidential personnel and financial data. The following applies to how users must interact with confidential personnel and financial data:

- Users must be advised of any confidential personnel and financial data they have been granted access. Such data must be marked or otherwise designated "confidential."

- Users must only access confidential personnel and financial data to perform their job function.

- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential personnel and financial information.

- Users must protect any confidential personnel and financial information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do their job or the action is approved by their supervisor.

- Users must report any suspected misuse or unauthorized disclosure of confidential personnel and financial information immediately to their supervisor.

4.5 Sharing Confidential Personnel and Financial Data with Third Parties

If confidential personnel and financial data, including cardholder data, is shared with third parties, such as service providers, a written agreement must govern the provider's use of the confidential personnel and financial information. The agreement must include the following: 1) an acknowledgement that the provider is responsible for the security of the data that it possesses, and that it will appropriately secure any data that it stores or transmits on behalf of the ORGANIZATION; and 2) how the data is to be used, transmitted, stored, destroyed.

When the ORGANIZATION will be sharing confidential personnel and financial data or cardholder data with a service provider or other third party, due diligence must always be performed prior to a provider being selected. ~~Further details about due diligence can be found in the Outsourcing Policy.~~

If media containing confidential personnel and financial or cardholder data is sent external to the ORGANIZATION, rigorous security procedures must be developed and maintained, which will include, at minimum, credential-verification and signature of the service courier. Media must be sent via a delivery method that allows the media to be tracked.

4.6 Receiving Confidential Personnel and Financial Data from Third Parties

If the ORGANIZATION receives or in any way handles confidential personnel and financial data for other entities, such as customers or partners, it must treat this data as if it were its own confidential personnel and financial data. The ORGANIZATION must acknowledge this responsibility in writing, through a formal agreement with the other entity. The ORGANIZATION must take all necessary steps to secure any data that it possesses, stores, processes, or transmits on behalf of its customers or partners that may affect the security of the entity's cardholder data environment.

Note: if the ORGANIZATION provides "shared hosting" services to its customers, it must also comply with additional PCI Data Security Standard requirements. These can be found in Appendix A of the PCI DSS (version 3.1), "Additional PCI DSS Requirements for Shared Hosting Providers."

4.7 Security Controls for Confidential Personnel and Financial Data

Confidential personnel and financial data requires additional security controls in order to ensure its integrity. The ORGANIZATION requires that the following guidelines are followed:

- Strong Encryption: Strong encryption must be used for confidential personnel and financial data transmitted external to the ORGANIZATION. Confidential personnel and financial data must always be stored in encrypted form, whether such storage occurs on a user system, server, laptop, or any other device that allows for data storage.

- Network Segmentation: The ORGANIZATION must use firewalls, access control lists, or other security controls to separate the confidential personnel and financial data from the rest of the corporate network. More information about this can be found in the Network Security Policy.

- Physical Security: Systems that contain confidential personnel and financial data, as well as confidential personnel and financial data in hardcopy form, must be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data.

- Printing: When printing confidential personnel and financial data the user must use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential personnel and financial data must be located in secured areas.

- Faxing: When faxing confidential personnel and financial data, users must use cover sheets that inform the recipient that the information is confidential. Faxes must be set to print a confirmation page after a fax is sent; and the user must attach this page to the confidential personnel and financial data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential personnel and financial data must be located in secured areas.

- Emailing: Confidential personnel and financial data must not be emailed inside or outside the ORGANIZATION without the use of strong encryption. More information can be found in the Email Policy.

- Mailing: If confidential personnel and financial information is sent outside the ORGANIZATION, the user must use a service that requires a signature for receipt of that information. When sent inside the ORGANIZATION, confidential personnel and financial data must be transported in sealed security envelopes marked "confidential."

- Wireless Access: When confidential personnel and financial data, such as cardholder information, is transmitted or accessed via wireless networks, the ORGANIZATION must use wireless industry best practices for encryption, such as IEEE 802.11i. Only the strongest encryption algorithms must be used to secure this data during transmission. Please note that the use of known insecure encryption methods, such as WEP, is expressly prohibited.

- Discussion: When confidential personnel and financial information is discussed it must be done in non-public places, and where the discussion cannot be overheard.

- Display: When confidential personnel and financial data is numerical, such as social security numbers or cardholder data, it must be removed if at all possible. If necessary for this information to be displayed, the number, such as a cardholder's Primary Account Number (PAN), it must be masked (i.e., such that only the last four digits displayed). Please note that this restriction does not apply to employees who must have access to this data to perform their job functions, however, the ORGANIZATION must ensure that only personnel who have a legitimate business need have access to the full PAN. This requirement does not supersede more restrictive requirements relating to the display of confidential personnel and financial data. Confidential personnel and financial data must be removed from documents unless its inclusion is absolutely necessary.

  If confidential personnel and financial data is written on a whiteboard or other physical presentation tool, the data must be erased immediately after the meeting is concluded.

- Media: Any media containing confidential personnel and financial information or cardholder data must be physically secured in an access-controlled area or high security zone. Media moved from one area to another must be logged with, at minimum, the following information: contact information of mover, reason for move, new location of media, security precaution taken, and proof of management approval was obtained prior to the media being moved. The ORGANIZATION must control all aspects of storage and accessibility of media, including storing media in secured areas, maintaining inventory logs of media, and conducting annual inventories of all media.

4.8 Applicability of Other Policies

This document is part of the ORGANIZATION's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

This policy will be enforced by the MVLS/SALS Joint Automation Information Security Manager and/or Executive Team. Violations will be reported to the member public library director and may result in suspension or restriction of access to all MVLS/SALS services. Where illegal activities or theft of ORGANIZATION property (physical or intellectual) are suspected, the ORGANIZATION may report such activities to the applicable authorities.

Appendix A: Policy Acceptance Form

[MVLS/SALS Joint Automation Project] is hereinafter referred to as "the ORGANIZATION."

I understand that being granted access to computer systems and ORGANIZATION information carries a great deal of responsibility. I recognize that I am being granted this access with the understanding that I will use the network resources and ORGANIZATION information in a responsible manner. I realize that specific guidelines and expectations of me are detailed in the appropriate policies.

I UNDERSTAND THAT WHILE THE ORGANIZATION INTENDS TO PROVIDE A SAFE AND POSITIVE EXPERIENCE WHEN USING ORGANIZATION SYSTEMS AND THE INTERNET, THE ORGANIZATION MAKES NO WARRANTIES AS TO THE CONTENT OF THE NETWORK AND THE INTERNET.

I AGREE THAT I AM RESPONSIBLE FOR MY OWN ACTIONS AND WILL RELEASE THE ORGANIZATION FROM ANY LIABILITY RELATING TO MY NETWORK USAGE. I AGREE TO USE THE NETWORK AND SYSTEMS IN AN APPROPRIATE MANNER AS SPECIFIED IN THE APPLICABLE POLICIES. I UNDERSTAND THAT MY USE OF THE NETWORK AND SYSTEMS MAY BE MONITORED AT ANY TIME AND I SHOULD HAVE NO EXPECTATION OF PRIVACY IN CONNECTION WITH THIS USE. I UNDERSTAND THAT I MAY BE GRANTED ACCESS TO CONFIDENTIAL INFORMATION AS PART OF MY ASSOCIATION WITH THE ORGANIZATION. I AGREE THAT I WILL A) ACCESS NO DATA THAT I AM NOT AUTHORIZED TO ACCESS, AND B) FOLLOW ALL APPLICABLE POLICIES THAT RELATE TO THE SECURITY AND PRIVACY OF THE ORGANIZATION'S CONFIDENTIAL INFORMATION.

I UNDERSTAND THAT FAILURE TO COMPLY WITH ORGANIZATION POLICIES MAY RESULT IN LOSS OF NETWORK PRIVILEGES, SUSPENSION, OR TERMINATION.

By initialing below, I agree that I have received, read, understand, and agree to the following policies:

_____	Acceptable Use	_____	Remote Access
_____	Password	_____	Confidential Library Patron Data
_____	Email	_____	Confidential Personnel & Financial Data

User Name (Print): _____

Signature and Date: _____