Sage Library System Information Security Policy

Introduction

Sage Library System seeks to ensure that appropriate measures are implemented to protect patron and employee personal and sensitive information. This Information Security Policy is designed to establish a foundation for an organizational culture of security.

The purpose of this policy is to clearly communicate the consortium's security objectives and guidelines to minimize the risk of internal and external threats. This policy covers two disparate groups of equipment. Those owned and managed by Sage Library System, as well as the workstations and infrastructure of Sage Library System Members. Sage Library System Member Organizations should have their own similar policies in place.

Compliance

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

Privileged Access

Access to the consortium's systems and applications above and beyond general user access shall be limited to the systems IT staff, contracted IT staff, and key administrators. VPN access through the firewall is required in order to access the servers themselves directly.

Data Backup & Recovery

The consortium will conduct regular backups of all critical business data. Snapshots of all Virtual Machines are automatically created nightly by the Eastern Oregon University IT department and stored on their servers. To ensure the database servers are appropriately backed up, all data is replicated in real time to the backup database server. In addition to that, both database servers run daily snapshots of the entire database to the Network Attached Storage (NAS) Device, as well as snapshots of all new data every 30 minutes. Confirmation that backups were performed successfully will be conducted regularly. The SageLib domain / web site is set to automatically back up and retain the most recent versions on the remote host's servers. Backups need to be downloaded quarterly and stored on the NAS.

Multi-factor Authentication

Multi-factor authentication is currently used to access the SageLib domain.

Endpoint Protection

All Sage Library System member workstations will utilize an endpoint protection tool to protect systems against malware and viruses. The servers themselves are protected by the firewall and therefore are exempt from this requirement.

Firewall with Security Services

The consortium will protect the corporate network from the Internet through the use of a firewall with Intrusion Prevention System (IPS) capability.

Email Security

All Sage Library System member workstations will protect their email systems by utilizing antivirus, anti-spam and anti-phishing technologies. They will also not utilize email to send or receive sensitive information.

Wireless
All Sage Library System members will set up their wireless utilizing two separate SSID's. One for organizationally owned devices and another for personal/guest devices. The password for the corporate SSID will not be shared with end-users and only known by key personnel.

Password Management
All staff accounts of Sage Library System and those of Sage Library System Members will follow the password configuration outlined in the Acceptable Use Policy below.

Acceptable Use Policy
Sage Library System will require all members to sign an acceptable use policy before accessing organizational resources. This policy governs the use of the consortium's resources and covers a wide range of issues surrounding the rights, responsibilities and privileges – as well as sanctions – connected with computer use. When your organization's Acceptable Use Policy differs from that of the Sage Library System member policy, you will need to follow whichever is stricter whenever feasible. See *Appendix A* for a copy of current Acceptable Use Policy

Asset Management
An inventory of all the consortium's hardware and software will be maintained that documents the following:
- Employee in possession of the hardware or software
- Location of hardware or software
- Date of purchase
- Serial number
- Type of device and description

Patch Management
All Sage Library System member workstations will be configured to automatically install software and operating system updates and patches. The Sage servers will have all server updates installed regularly, preferably monthly.

Securing Remote Workers
The consortium requires all remote users to utilize consortium owned devices when working remotely. Those devices will be set up with a secure VPN.

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

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

Incident Response

The consortium will utilize an incident response plan in the event of a cyber related incident. This plan will include at the minimum:

- Essential contact for an incident response service provider, FBI, local law enforcement, cyber insurance company, legal counsel.
- Users roles and responsibilities.
- Schedule of regular testing of the incident response plan.

Auditing and Logging

The consortium will ensure proper logging is enabled on all critical resources. Access logs showing where database queries originated through the OPAC are automatically logged on the Application servers. They have been set to show originating external IP addresses whenever possible to allow blocking of traffic should inappropriate behavior be detected. All stuck database queries are logged automatically for later analysis. All other servers have logging enabled to assist with troubleshooting.

Appendix A – Acceptable Use Policy

Purpose
The purpose of this policy is to outline the acceptable use of the Sage Library System ILS. This policy will also cover acceptable use of computer equipment, email, and internet access throughout Sage Library System member organizations, as well as any equipment owned by Sage Library System itself. These rules are in place to protect the employee, members and consortium. Inappropriate use exposes the consortium to risks including virus attacks, compromises of network systems and services, and legal issues.

Scope
This policy applies to both permanent and temporary employees of the consortium. This policy applies to all equipment that is owned or leased by the consortium. This policy is a supplement to the Sage Library System Information Security Policy and provides guidance for Sage Library System Member Organizations in regard to their own IT infrastructure.

General Use
IDs/Passwords:

All Sage Library System member ILS accounts will utilize the following password configuration:

- Staff account inactivity lockout threshold: 60 Minutes
- Minimum password length: 12
- Maximum password age: 365 days

In addition, Sage Library System members will educate users on creating/utilizing secure passwords for systems/services that can't be controlled by the consortium. Use of a password management utility is strongly recommended.

Access to the consortium's IT systems are controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on consortium owned systems and services.

Password Requirements for Sage Library System owned workstations and servers:

- Minimum password length: 12
- Must have a combination of letters, numbers, and special characters.
- If possible, utilize a password manager to create (much stronger) and unique passwords for each service or account.

Individuals must not:

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

Internet Use

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

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

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

Email:

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

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

Clean Desk and Clear Screen

In order to reduce the risk of unauthorized access or loss of information, the consortium enforces a clear desk and screen policy as follows:

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

Working Off-site

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

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

Mobile Devices

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

Mobile Storage Devices

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

Telephone Equipment Conditions of Use

The use of organizational voice equipment is intended for business use. Personal use of voice equipment is allowed but should be limited. Individuals must not:

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

Actions upon Termination of Contract

All organizational equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the consortium at termination of contract.

All data or intellectual property developed or gained during the period of employment remains the property of Sage Library System and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

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

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

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

Signature

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

_____

(Print your name)

_____ _____

(Signature) (Date)