Archdiocese of Seattle (CCAS)

Security System Management Policy

Final

January 2024

Table of Contents

Security System Management Policy

Summary

The purpose of this policy is to set the minimum guidelines necessary to make sure that the confidentiality, integrity, and availability of data on the Corporation of the Catholic Archbishop of Seattle (Archdiocese) network assets are protected from malicious software, cyber criminals or accidental disclosure or loss of sensitive information. To do this, we deploy security software and policies on all systems of the Archdiocese network as set of mandatory standards.

This policy applies to all on-premise and cloud computing and network platforms and systems owned, licensed, contracted, leased, or operated by the Archdiocese (collectively, "resources" or the

"Archdiocese Network" or "network"). This includes all parishes, schools, and cemeteries in the Archdiocese. It may also apply to personally owned or third-party computers transmitting our sensitive data electronically or connecting directly to the Archdiocese Network, including any websites operated by us.

This policy applies throughout the organization as part of the Archdiocese Security Program. It is particularly relevant to IT users and administrators, including, as applicable, all administrative consultants, employees, contractors, and third parties who are affiliated with or use or access the Archdiocese Network (collectively, "Users").

Implementation of the Security System Management Policy is the responsibility of the Location IT Support. For the Chancery, the IT Services department is the responsibility of Information Technology Services. For parishes, schools and cemeteries, Location IT Support is the responsibility of the employee or contracted service identified to support the local Computing Resources by the Location Administrative Leader. The Location Administrative Leader may be a pastoral assistant, principal or other designee by the pastor or Archbishop.

Where an outsourced or hosted solution is relied upon to a significant extent, CCAS requires as reasonably available, a System and Organization Controls (SOC) for Service Organizations internal control report. The report should be prepared according to the standards established by the American Institute of Certified Public Accountants (AICPA) including independent attestation. This is required so that CCAS can examine risk associated with services provided by an outsourced service.

The CCAS Security System Management Policy includes the following:

- Virus and Malicious Software Protections
- Encryption
- Social Engineering and Scamming Protections (i.e. Phishing)
- Physical Security Protocols
- Data Retention and Backup Protocols
- Security Operations
    - Logging and Event Monitoring
    - Patching and Vulnerability Management
    - License and Asset Management
- Security Incident Response Protocols

Virus and Malicious Software Protections

Knowing and willful introduction of a computer virus, malware, and disruptive/destructive code to the Archdiocese Network is prohibited.

Users are not to make any changes to their system that will disable or remove Archdiocese approved antivirus and malware prevention software or otherwise prevent the software from performing its intended purpose.

Users are not to download or open any software, files or macros attached to an email from an unknown, suspicious, or untrustworthy source. All unexpected content received from a trusted source should be verified with that source prior to opening. Users who discover or suspect virus or malware incidents must report them immediately to their respective Location IT support team.

Computer systems that are unable to run antivirus and malware prevention software must be restricted to an isolated network with sufficient network-level protections deployed to prevent viruses/malware from spreading into any other areas of our network (e.g., running antivirus technology at its "gateway" to the Archdiocese Network).

The Location Support is responsible for deploying and maintaining approved antivirus/malware prevention software to all systems it supports/administers and for providing timely updates for all components of the software on:

- any externally facing servers or gateways; ii. proxy servers; iii. application servers such as mail servers and/or mail gateways, FTP servers, web servers, audio/video servers; iv. data management servers such as back-up servers and database servers.
- Archdiocese deployed hardware resources such as desktops, laptops, and tablets.
- when technically feasible, cell phones, smart phones and PDAs
- for non-Archdiocese deployed laptops or mobile devices accessing CCAS Computing Resources.

Location IT Support should ensure that both up-to-date antivirus/malware prevention software and a personal firewall are deployed on the connecting device prior to granting permission to connect to the Archdiocese Network.   All devices with an IP have an operating system that needs routine evaluation for security vulnerabilities frequently (e.g. monthly).

Antivirus/malware prevention updates will be installed and scheduled to run at regular intervals or upon electronic notification of a new security update, patch, vulnerability, or threat. Wherever possible, computing resources will be set to auto-apply/update security patches on a regular basis.

Antivirus and malware prevention scanning should be programmed to run/initiate upon startup and/or reboot of PCs/servers/other computing devices.

For PCs/servers/computing devices that are not normally rebooted, antivirus and malware scanning should be "always on" when technically feasible. If not possible, Location IT Support should ensure that antivirus and malware remediation is accomplished for the protection of our electronic assets. User may not disable these protections on any Archdiocesan device.

Location IT Support is responsible for monitoring, receiving, and acting upon alerts (via automated alert, email, news, etc.) promptly to ensure minimal exposure and security risk to the confidentiality, integrity, and availability of our electronic assets.

Critical security patches should be deployed by Location IT Support a maximum of 48 hours after release by the operating system software or application vendor unless there is reason to believe the patch might negatively impact a business-related activity or application. E.g., After appropriate testing, updates without issue will be made available to all PCs/servers/computing devices/network equipment/appliances, as well as to devices utilized by remote employees. Best efforts will be made to notify users of implementation of critical patches.

Location IT Support will run malware prevention software scans routinely (at a minimum weekly).

Location IT Support will run antivirus and malware prevention software immediately after the installation of any new software, not normally supported by Location IT

Suspicious content (files or macros attached to email) will be quarantined for review or permanently deleted immediately.

All downloads should be scanned with an updated Archdiocese standard antivirus/malware prevention scanner immediately (automatically, if possible).

Computing systems will be rebooted as required to ensure virus definitions (as well as operating system updates) are updated and that the antivirus software can run to check for viruses.

Encryption

When CCAS Confidential, Highly Restricted or PHI (HIPAA) information is transmitted over any communication network, it must be sent in encrypted form. Whenever Archdiocesan source code, or source code that has been entrusted to the Archdiocese by a business partner, is to be sent over a network, it too must be in encrypted form. Specific definitions of the words "Confidential" and "Highly Restricted" can be found in the Information Classification Policy.

All Archdiocese Confidential or Highly Restricted information stored on backup computer media must be encrypted using approved encrypting methods.

Whenever Highly Restricted information is not being actively used, it must be stored in encrypted form. This means that when this information is stored or transported in computer-readable storage media, it must be in encrypted form. Additional information related to the storage of Highly Restricted information can be found in the Information Classification Policy.

Encryption of information in storage or in transit (including email) must be achieved through commercially available products approved by the CISO.

Whenever encryption is used, users must not delete the sole readable version of the information unless they have demonstrated that the decryption process is able to reestablish a readable version of the information.

Encryption keys used for Archdiocese information are always classified as Confidential or Highly Restricted information. Access to such keys must be limited only to those who have a need to know. Unless the approval of the CISO is obtained, encryption keys must not be revealed to consultants, contractors, temporaries, or other third parties. Encryption keys always must be encrypted when sent over a network.

Whenever such facilities are commercially available, the Location IT Support must employ automated rather than manual encryption key management processes for the protection of information on Chancery networks.

Data and Program Backup

All information and data files, including sensitive information such as Highly Restricted, Confidential, or Internal Use Only resident on the Archdiocese networks must be stored on Location servers or cloud services and regularly backed up. User department supervisors must advise Location IT Support which information is to be backed up. Location IT Support will perform full backups on all servers and cloud storage every night. If required, additional backups will be taken for operational and business reasons.

Personal computer users must store their data files on the Archdiocesan Network as specified by Location IT Support so they can be backed up. Portable computer users must synchronize their files with any changed or new files since their last logon session on the Archdiocesan Network.

The preferred approach for backup will be to Cloud storage services. This includes cloud storage and on-premise storage. Backup is the responsibility of Technical Support.

Web sites, Web pages, and e-mail are records, and are subject to the same legal, administrative, historical, fiscal, and canonical principles of retention and disposition as records in paper and other formats. Unless the type of information is specifically listed on the Archdiocese Information Retention Schedule, available from the Chancellor's Office, information must be retained for as long as necessary but for no longer. Information listed on the Information Retention Schedule must be retained for the period specified. Other information must be destroyed when no longer needed, which is generally within two years.

Department supervisors are strongly encouraged to prepare and periodically update Location contingency plans to be able to restore service for all production applications, despite whether internal network services are required for the support of these applications. The Location IT Support is responsible for preparing and periodically updating network service contingency plans. Each Location is responsible for the periodic review of these same contingency plans, including the review of tests performed to validate those contingency plans.

Logs and Other Systems Security Tools

Every significant component of the Archdiocese Network must include sufficient automated tools to assist the Location IT Support in verifying a system's security status. These tools must include mechanisms for the recording, detection, and correction of commonly encountered security problems.

Whenever cost justifiable, automated tools for handling common security problems must be used on Archdiocese Network. For example, software that automatically checks personal computer software licenses must be used regularly.

To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical Archdiocese information must securely log all significant security relevant events. Examples of security relevant events include users switching user IDs during an online session, attempts to guess passphrases including multiple login attempts, attempts to use privileges that have not been authorized, modifications to production application software, modifications to system software, changes to user privileges, and changes to logging system configurations.

Logs containing computer or communications system security relevant events must be retained by Location IT Support for at least three months. During this period, logs must be secured such that they cannot be modified, and such that only authorized persons can read them.

Certain information must be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information must be securely stored offline until it is determined that the Archdiocese will not pursue legal action or use it. The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, and copies of all potentially involved files.

Records reflecting relevant security events will be periodically reviewed in a timely manner by the Location IT Support and the CISO as necessary. Location IT Support will review security logs of multiple login attempts at least weekly and will upon finding probable cause for concern, notify the CISO immediately. They will also take any necessary steps to track down, identify and isolate potential security breaches. Logs containing information on the activity concerned will be retained for a sufficient time to ensure they are not destroyed before a complete and formal analysis has run its course.

The CISO will inform users of specific acts that constitute computer and network security violations. Users will also be informed that such violations will be logged.

Patching and Vulnerability Management

Location IT Support are required to promptly apply all security patches to the operating system that have been released by knowledgeable and trusted user groups, well-known systems security authorities, or the operating system vendor. Only those systems security tools supplied by these sources or by commercial software organizations may be used on the Archdiocesan Network. Users are expected to comply with software patching requirements as deemed necessary and distributed by the respective IT function.

Perimeter Defense Standards and Procedures

Firewalls are to be used to separate networks with differing security requirements, such as the Internet and an internal network that houses servers with sensitive data. Locations should use firewalls wherever their internal networks and systems interface with external networks and systems, and where security requirements vary among their internal networks.

- A Location’s firewall(s) placement on the network and policy should be based on a comprehensive risk analysis.
- Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic.
- Firewall Policies should consider the source and destination of the traffic in addition to the content.
- Many types of traffic, such as that with invalid or private addresses, should be blocked by default.
- Locations should have policies for handling incoming and outgoing IPv6 traffic.
- Locations should determine which applications may send traffic into or out of its network and make firewall policies to block traffic for other applications. ￼

Security Incident Response Plan

The purpose of this Incident Response Plan (“IRP”) is to provide guidance on the appropriate steps to be taken and documented in the event of a possible security incident or data breach, from the time of suspected breach to post-incident response closure, so that all incidents are handled in a consistent manner and the exposure to the potentially breached party is limited. It also provides a methodology for collecting evidence in the event of criminal activity. Documentation of responsive actions taken in connection with any security incident or data breach, as well as documentation of the post-incident events and actions taken, is critical in making appropriate changes to business practices to improve the safeguarding and handling of Archdiocese Sensitive Information and PII[1]. The IRP is part of an overall Archdiocesan Information Security Policy (ISP)

This IRP process applies to all employees of the Archdiocese of Seattle, including parishes, schools, the Chancery, and associated entities. The IRP also applies to consultants, contractors, temporary personnel, and the like who may experience or witness a security incident or possible data breach while working for the Archdiocese of Seattle. After discovery, this process provides Chancery Information Technology or Location IT resources with a checklist for responding so that steps or information related to the incident are not missed. We are committed to protecting our information and responding appropriately to a security incident or data breach.

Definitions

Chief Information Security Officer (CISO) – Designated employee responsible for information and data security for the Archdiocese of Seattle.

Chancery Information Technology – Information Technology professionals responsible for support of Chancery IT assets.

Location IT resources – Contract, volunteer or employed technology professionals responsible for the technical support of parish or school IT assets.

Location Leadership – For parishes, typically the leaders would be the Pastor, Principal or Pastoral Associate for Administration.

Incident Leader – For every security/data breach, an Incident Leader will be identified. Usually, the Incident Leader would be the CISO at the Chancery (or designee) and Location Leadership (or designee) for schools and parishes.

Incident Response Team – Designated by the Incident Leader to perform the diagnostic and remediation activities related to an incident. Typically, this would be the Location IT resources or the Chancery Information Technologies staff.

Roles and Responsibilities for Security and Data Breach Incident Response

Employees/Contract staff – Employees, volunteers with access and any contracted staff are responsible for identifying actual or potential breaches of security or data and notifying their supervisor and Location IT resources. Chancery staff should contact the Help Desk (helpdesk@seattlearch.org) and their supervisor.

Location Leadership – Responsible for coordinating the overall local response to actual and potential security and data breaches, including allocating Location IT Support resources, employees, and local resources. They are the Incident Leader for a security/data breach at a location unless otherwise determined.

Incident Response Team – Location IT Support resources responsible for performing initial technical response to a potential and/or actual Security/Data Breach. The response includes technical activities to contain the breach, assess damage and risk, prevent further harm, recover any lost data or asset(s) and preserve evidence. The response may be performed by local technical staff and/or in conjunction with third party resource(s) as needed.

Chief Information Security Officer (CISO) – The CISO is responsible for keeping the Incident Response Plan up to date. They work with legal, risk management, and operations leaders to make sure the IRP meets the organization's needs. They may serve as the Incident Leader on large scale security/data breaches.

Incident Leader - Responsible for following the Incident Response Plan, completing activities from the Incident Response Checklist, and completing the Incident Response and Incident Closure Forms. They will be appointed by the Location Leadership.

Location Leadership, Incident Response Team, CISO and Incident Leader, should be identified with backups identified too.

Scope

Protection of our information and data is paramount. This Cybersecurity and Data Breach Incident Response Plan (IRP) provides a checklist[2] for responding to a security incident or potential data breach. An incident can be intentional or unintentional, and this IRP could be implemented in response to many events having an adverse effect on the Archdiocese.

Guidelines

This IRP describes our response to potential and actual breaches of network and data security. CCAS is interested in potential breaches of sensitive information, including Personal Identifiable Information (PII) PII can include name, address, social security number or other identifying number or code, telephone number, email address, or etc. f. We are responsible for protecting the confidentiality, integrity, and availability of and both Archdiocesan data and other technology assets. This IRP is used to:

- Help determine if a breach occurred.
- Guide the response to the potential breach including containment, recovery and potential notification of parties impacted and law enforcement.
- Conduct a reasonable investigation to determine the likelihood of information that has been or will be misused.
- Provide guidance on meeting state and federal guidelines and requirements for notification.
- Conduct a post-incident investigation to capture lessons learned.

The IRP should be tested annually by location leadership to ensure all participants on the Incident Response Team (IRT) know their roles in the event of a true incident.

IRP Contents

- How do I know if there has been a security or data breach? - Assistance in determining if a security or data breach has occurred.
- Incident Response Checklist/Form – Checklist for responding to incidents. It also provides a way of documenting the details of a potential or actual security/data breach.

- Incident Closure Form – Form for documenting the key results and learnings of an actual security/data breach.

How do I know if there has been a security incident or data breach?

If any of the following happen, a security or data breach may have occurred:

- Staff receive an unusual email with a link or attachment that they subsequently have clicked on.
- Staff get a ransomware message.
- Staff get a fake antivirus message.
- Staff have unwanted browser toolbars.
- Staff internet searches are redirected in unexpected ways. For example, it is common to redirect all internet searches within an organization to "safe search" services (Google Safe Search, etc.). This would be an anticipated redirect. A sudden change of search engine to a product no one is familiar with would not be.
- Staff see frequent, random popups.
- Staff member's friends receive social media invitations from staff member that they did not send.
- Staff's online passphrase isn't working.
- Staff observe unexpected software installations.
- Staff mouse moves between programs and makes selections without user input or being aware that an approved resource (Chancery IT, parish/school computer support staff) are providing remote assistance.
- Antimalware, antivirus, Task Manager, or Registry Editor is disabled.
- Staff/parish/school online banking account is missing money.
- Staff have been notified by someone that they have been hacked.
- Confidential data has been leaked.
- Staff observe strange network traffic patterns.
- Staff device is stolen.
- The presence of pornography.
- Generation of unknown/unexpected new accounts, either on local or network resources.

Compliance

Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. The Archdiocese reserves the right to advise appropriate authorities of any violation of law.[3]

Exceptions

Any exceptions must be approved by the CISO and General Counsel.