Archdiocese of Seattle (CCAS)

Information Security Program

Final

January 2024

Table of Contents

Information Security Program

The purpose of this Information Security Program ("ISP") is to provide a security framework that will ensure the protection, confidentiality, integrity, and availability of Archdiocese of Seattle information assets, physical assets, Archdiocesan information, parishioner and employee information (collectively, “Archdiocese Assets”). The ISP should also help ensure compliance with all applicable state and federal laws applying to privacy and personal information. All policies and standards should be consistent with teachings of the Catholic Church. Standards and procedures related to this ISP will be developed and published separately.

The ISP applies to the following entities within the Corporation of the Catholic Archbishop of Seattle, Chancery, Parishes, Parish Schools, and High Schools, Fulcrum, St. Joseph Foundation, WSCC and Cemeteries.

The ISP applies to all employees, contractors, consultants, temporaries, volunteers, and other users across the Archdiocese, including those users affiliated with third party vendors who access the

Archdiocese computing environment. Throughout this policy, the word “user” will be used to collectively refer to all such individuals.

The ISP also fits into the overall Risk Management oversight of the Archdiocese. The Program will include the following elements:

1. Information security policies and procedures to provide for the confidentiality, integrity, and availability of Company Assets including the internet, hardware, software and other technology provided or licensed (“resources”) by The Archdiocese of Seattle, including the Chancery, parishes and schools (“CCAS”).
2. Computer access controls, including the identification, credentialing and authentication of employees, administrative consultants, contractors, non-employees, and clients; 1 Such a team should be formally established with named employees (non-contractors) and empowered with the necessary authority to enforce this policy.
3. An incident response plan ("IRP") to address possible security incidents 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.
4. Mobile computing standards and controls for access of data regardless of location.
5. Risk Assessments conducted at least every three years, or upon completion of a major system change or as a requirement of the cyber insurance carrier(s). Consideration should be given to periodic risk assessments by a third party.
6. Investigation of identified or suspected misconduct, policy violation, or criminal acts as conducted or suspected to be conducted with aspects of the IT infrastructure. Maintain available investigators who are competent, current, resourced, and prepared to provide timely and thorough investigations and findings, independently or in cooperation with law enforcement or regulatory agencies. These qualified persons may be third parties.
7. Security Awareness Training and Education which emphasizes the importance of protecting Archdiocesan Sensitive Information and personally identifiable information ("PII") during different states, as well as how and when to report a potential security breach or incident to Information Security.
8. Monitoring and auditing of all aspects of the use and implementation of, and compliance with, the ISP by locations including schools, parishes, and the Chancery.
    - 8.1. Annually revisiting Information Security policies and procedures for changes in laws, as well as technology and standards change.
    - 8.2. Support the Human Resources Department with ensuring continuity between the ISP and its operating procedures, such as background investigations, terminations, computer breaches, fraud, embezzlement, unlawful acts or other forms of dishonesty and violations of our policies.

Summary and Overview

Framework

A framework of policies is the foundation for any IT security program. Given the amount of change and transformation in the technologies employed and used by CCAS over the last 1-2 years and the introduction of remote/hybrid work this framework is being updated to solidify that foundation. In this revision, updates/changes are being made where provisions are no longer relevant and new provisions are being added in consideration of where the environment changed significantly. In addition to the individual changes made, the following high-level framework is proposed to simplify and facilitate the review and adoption of these updated policies:

- **Acceptable Use:** This policy is the cornerstone of the framework with an intended **audience of all-users**. The intention and purpose of this policy is to do the following:
    - establish a clear set of boundaries and expectations for everyone using the organization’s IT resources (incl. clear delineation of the subsidiary or component(s) within CCAS to which the policy should apply),
    - declarations of the need to always comply with use and copyright laws, including appropriate use of software and copyrighted material.
    - declares the degree to which the policy is enforceable and outlines consequences for violations of these provisions.
    - state that users are personally responsible and potentially liable for actions taken when connected to the network or internet,
    - states the intended use of these IT resources is for the benefit of the organization and the furthering of its mission,
    - provide a code of conduct governing user behavior and
    - statements or notices the policy complies with state, national or church/canon rules and regulations (should it indeed be).
    - statements or advice that users are responsible for their own personal safety and privacy while using the internet.
    - notifications of limitation of liability (safeguarding against errors and omissions)
    - position the resources as a tool with responsibilities.
    - use of email (including the email/communications policy) and file sharing systems – facilitate collaboration and need to know – standardization – consistency.
    - Establishes endpoint device management standards for
        - CCAS-Owned IT Assets
        - Devices owned by individual personnel (BYOD) – when working remotely – you agree to be reachable as a requirement/allows some degree of manageability; email/productivity – privilege.

- **Data Classification (audience = IT):** A good data classification policy provides a productive and neutral zone of demarcation in the environment and rationalizes the exchange of needs and service among IT, business/departmental and application owners. This policy is noticeably unapparent or missing entirely from the CCAS framework and should be implemented post-haste. A data classification standard will provide a tool for which the categorization of data is enabled and will help CCAS to effectively and clearly answer the following questions:
    - What are the various types of data available in the environment?
    - Where are certain data located?
    - What access levels are implemented?
    - What protection level is implemented and does it adhere to compliance regulations?

Further study of the data in the environment will need to be conducted to inform and implement this policy. Known examples of data types that are apparent today include financial, personnel, archival, tribunal/pastoral, legal processes, and work product, etc. among many others that should be enumerated. Implementation of this policy will be successful when employees and affiliates are able to recognize each type of data AND use the proper handling protocols when working with or interacting with that data.

Finally, the data classification standard will bring together relevant compliance requirements of the organization and address, for all, the degree to which they are in-scope and relevant (i.e. PCI, PII, HIPAA, CIPA, SOX, etc..).

- **Technology Access (incl. remote/endpoint and use of personal devices) (audience = IT):** This policy defines the organization's information security principles and requirements for connecting to its network and compute resources from any device from any endpoint. Considering the recent cloud migration, the updates to this policy should yield some interesting conversations. For example, take the following into consideration:
    - There is now a considerable amount of the CCAS compute resources and business applications being managed by 3P cloud-hosted software solution providers. Little remains in terms of on-premises and local IT managed compute resources.
    - The advent of remote and hybrid working arrangements has created new service demands for IT (upgraded WiFi, increased usage of VPN, increased demand mobile devices access, 1:M user to device authentication/usage, etc.

  The access policy should include the following provisions:

    - Outline the process for granting, reviewing (new/needed) and revoking/termination/suspension access.
    - Establish least-privilege and role-based access as the standards for control.
    - Establish edge-of-network access and authorization controls (IEEE 802.1x with IT managed personal credentials/certificate).
    - Establish passphrase access controls.
    - Establish Zero trust as target principle.
    - Establish inactivity, lock screen, and unattended controls.
    - Establish multi-factor authentication as a standard access control.
    - Establish SSL by either HTTPS (onus IT) or VPN as a standard access control.
    - Establish standards for use of data encryption and transmission of data.
    - Establish controls for administrator and super-user access (incl. passphrase mgmt. tools)
    - Management and control of third parties

- **Security System Management Policy (audience = IT):** IT security management is perpetual process of identifying, protecting, and maintaining the organization's assets, including data, information, IT infrastructure (including network infrastructure) and IT services or collectively, IT resources. The goal of IT security management is to ensure the availability, integrity, and confidentiality of these assets and resources. The following elements should be addressed in this policy group:
    - Establish a published baseline configuration and process for change control.
    - Oversight and Governance, Accountability

  - Virus Scan and Malware Protection
  - Phishing Protection
  - Physical Security Protocols
  - Data and Program Retention and Backup (not to overlap or conflict with archival)
  - Logging and Event Monitoring
  - Patching and Vulnerability Monitoring, Reporting (including zero-day vulnerabilities)
  - License and asset management
  - Incident or breach response procedures and protocols (incl. Communication

Oversight

The oversight of the Information Security Program is the responsibility of the Archdiocesan Finance Council (AFC). The AFC has delegated the ISP to the Technology Committee and its Security Committee.

Any and all revisions to this policy must be reviewed and approved by the Security Committee.

Security Committee Roles and Responsibilities

- Provide oversight to the Information Security Program.
- Perform Annual Risk assessment for the Archdiocese.
- Identify priorities for reducing risk associated with information security.
- Review and update associated policies on a periodic basis.
- Help ensure compliance with state and federal privacy and security laws.

Security Committee Membership

- Chair – Chief Information Security Officer
- Archdiocesan Risk Manager
- Archdiocesan Counsel
- Human Resource representative
- Parish Representative
- School Representative
- Archive Representative
- Chancery IT Security staff
- Parish Financial Services
- Archdiocesan Finance Counsel appointee
- Appointed volunteer industry experts

Roles and Responsibilities

- **Chief Information Security Officer (CISO)** – Professional responsible for developing, implementing and enforcing security policies. Responsible for communication security policies to technical and non-technical staff. Also responsible for security oversight committee, ensuring the security operations structures support the policies. Responsible for Risk management, audits and security compliance across the Archdiocese. Will be involved in high level incident response.

- **Location Information Technology Support** – Technical staff responsible for the technical implementation of the security policies at the locations across the Archdiocese. They are also responsible for monitoring compliance with policy and first level incident response.
- **Location Administrative Leader** - (see definition in the glossary) Responsible for the overall compliance with security policies and to support and hold local technical support accountable for the technical implementation of policies. They are also responsible for the education of all staff on the risks and responsibilities of using Archdiocesan computing resources.

General Policy

All information traveling over CCAS computer networks that has not been specifically identified as the property of other parties will be treated as though it is an Archdiocese corporate asset. It is the policy of the CCAS to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. In addition, it is the policy of the CCAS to protect information belonging to third party vendors that have been entrusted to the CCAS in a manner consistent with its sensitivity and in accordance with all applicable agreements.

Location Policies

Locations (parishes, schools) may have local policies and procedures. They should be reflective of local needs and risks. Location specific policies should be consistent where as much as possible. Where gaps in location policy exist or policies exist that conflict with this ISP, the ISP and its related polices take precedence.

Violations

Users who willingly and deliberately violate this policy will maybe subject to disciplinary action up to and including termination.

Glossary

Location – Chancery, parish, school or cemetery where CCAS activities may take place.

Location IT Support – The department, employee or contracted personnel that provides support at a location. For the chancery, the Location IT Support is the IT Services department.

Location Administrative Leader - The Location Administrative Leader may be a pastor, pastoral coordinator, pastoral assistant, principal, executive, director or other person designated by the pastor or Archbishop.

Computing Resources – End user devices, servers, appliances, network, cloud services, Software as a Service.

CCAS Confidential, Highly Restricted or PHI (HIPAA) information

Archdiocesan Network – Network hardware, wiring and appliances used to access Computing resources.