Archdiocese of Seattle (CCAS)

Technology Access Policy

Final

January 2024

Table of Contents

1

Technology Access Policy

Summary

The Access Control Policy is intended to protect the Archdiocese from unauthorized use of network and system resources and data. In addition, the policy protects the integrity, availability and confidentiality of Archdiocesan networks, systems, and data.

This policy establishes the minimum standards to be implemented and sustained across all CCAS sites and locations. Location (i.e., School, Parish, Chancery or Cemetery where the Archdiocese conducts its mission) specific procedures or standards may not enforce a lower standard or conflict with this policy; however, they can enforce a higher or stricter standard. Access controls need to match the sensitivity of the data or resource to be protected.

The policy applies the internet, hardware, software (including Software as a Service) and other technology provided or licensed ("resources") by The Archdiocese of Seattle, including the Chancery, parishes and schools ("CCAS"). These resources are provided for employees and authorized persons affiliated with CCAS ("users").

Authorization

Users of Archdiocesan resources will be given the least-privilege access needed to efficiently perform their duties. The person who manages access for a resource needs to approve changes to that access. Changes include adding or removing access. Every change needs a valid business justification. For example, access to a resource may require approval by:

- a user's supervisor,
- an access request coordinator, and
- the data owner or another person with authority to grant access to the specific data.

CCAS requires each user to have a unique ID to authenticate with. Users must keep these ID's safe and make sure they are used only by the person they are assigned to. People who handle this work must enforce those policy requirements by holding users accountable if they do not follow the rules.

Role Based Access will be implemented where technically possible. Role based access provides permissions to system resources based on job role. Changes to any role permissions requires approval by the person who manages that role.

When third parties need access to a resource, access must go through an approval process. A person who manages technology for the system and an owner of the data are the correct approvers. Third party access will be limited to a period needed to accomplish the required tasks. These users must complete with IT policies and compliance standards.

IT staff use of administrative and system technical support accounts must be approved by (at a minimum) those responsible for managing the resource. This may be an IT Director or location leader or their delegate. Every system and service account must have a designated person responsible. If that person changes, a new person must be named.

Audit and Review

People who approve access to a resource must also approve all modifications and periodically review as well. These responsibilities include:

- Keeping access approval and review records current so they accurately reflect each person's role and the access they need according to the principle of least-privilege.
- Making sure to carefully follow HR procedures to handle employee suspensions, terminations, and transfers. Take steps to revoke access privileges when those changes happen.
- Revoking access when it is no longer needed or proper.
- Promptly reporting any possible or actual unauthorized access to Location IT support or location leadership and following the Information Security Incident Management Standard and other policies that may apply to the data or system.
- Taking action when any other possible Information Security Incident is identified. Users must notify Location IT support immediately.

Revoking Resource Privileges

CCAS requires an official and repeatable process for offboarding employees who have left the organization. The process will ensure all resource access is disabled, keys are returned, and owned devices are returned.

When a change in user duties or employment status occurs that person's supervisor must promptly inform Location IT Support responsible for user IDs. Human Resources also must issue a notice of status change to the data owner as well as Location IT Support who might be responsible for the resources on which the involved user might have a user ID.

All user IDs should have the associated privileges revoked after a certain period of inactivity not exceeding 30 days.

Access Control

Any endpoint resource that connects to any other CCAS resource must use passphrase-based access controls including multi-factor authentication (MFA). Exceptions would include public wireless networks provided for parishioners or visitors to the Location. Such public networks should be entirely separate from the secure network used to perform normal operations of a Location. Each passphrase should meet the following minimum standards:

- Locations with MFA implemented should have minimum 15-character length requirement for passphrases.
- Locations without MFA should have minimum 17-character length requirement for passphrases.
- All passphrases should include special characters, numbers and both upper- and lower-case letters.
- Passphrases should be changed annually.
-
- Similar/Repeat: May not be identical or similar to previous passphrases.
- No Readable Form: Passphrases must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in data communications software, in web browsers, on hard drives, or in other locations where unauthorized persons might discover them.
- Not Written Down: Passphrases must not be written down and left in a place where unauthorized persons might discover them. Aside from initial passphrase and passphrase-reset, if there is reason to believe that a passphrase has been disclosed to someone other than the authorized user, the passphrase must be changed immediately.
- Never Shared: Passphrases must never be shared or revealed to anyone else besides the authorized user. Default initial passphrases, which are used for new user ID assignment or password reset situations should be immediately changed.
- All passphrases must be changed immediately if they are suspected of being disclosed or known to have been disclosed to anyone other than the authorized user. Location IT support may reset a user at any time.
- Access to Location managed Computing Resources or any Cloud Based Computing Resource from a non-trusted site should be through an authenticated and encrypted connection such as a VPN or SSL browser session (https://...).
- Positive Identification: All users must be positively identified prior to being able to use any resource. Positive identification for a resource involves the combination of a user ID and fixed passphrase, both of which are unique to an individual user.

Multi-Factor Authentication

CCAS requires resources accessible from a network not managed by CCAS, so use MFA. Resources requiring the use of multi-factor authentication include, but are not limited, to virtual private network (VPN), systems utilizing Single Sign-On (SSO), hosted applications, system administration tools, and privileged accounts.

Inactivity & Automatic Logoff

Users must not leave their personal computer, workstation, or terminal unattended without logging out, locking the workstation, or invoking a protected screen saver. A screen saver program must automatically blank the screen and suspend the session if there has been no activity on a resource for a certain time. Re-establishment of the session must take place only after the user has provided a valid passphrase. The recommended maximum period is 15 minutes, but Location IT Support may set a shorter duration.