_TEST_Pages_

1100 Electronic Records Management Policy v2

October 17, 2024October 21, 2024

1100 ELECTRONIC RECORDS MANAGEMENT POLICY

1100.1 Purpose:

The purpose of this Electronic Records Management Policy is to establish guidelines and procedures for the backing up certain electronic records, as well as the retention and destruction of
any such backup by the Archdiocese of Baltimore.

1100.2 Scope:

This Policy applies to electronic records that are stored on computer servers owned, leased, or provisioned at third-party hosting facilities and maintained or managed by the Archdiocese of Baltimore technology department.

1100.3 Electronic Records are Archdiocesan Property:

All electronic records generated or received by the Archdiocese are the property of the Archdiocese. Employees do not have any personal or property rights to records, electronic or otherwise, created, received, or generated on behalf of the Archdiocese. Similarly, no third party storage facility or entity has any personal or property rights to records, electronic or otherwise, stored by the Archdiocese at or with any such facility or entity.

1100.4 Definitions:

4.1. Electronic Record

An Electronic Record includes recorded information, regardless of medium or characteristic, which is stored on a physical or virtual computer server owned or leased maintained by the Archdiocese.

4.2. Records Hold

A Records Hold is the cessation of destruction of any records that relate to the subject of the Records Hold.

4.3. Backup

A Backup, or the process of backing up, refers to the copying and archiving of computer data for later retrieval.

1100.5 Backup and Retention:

5.1 Enforcement and Implementation

The Director of Information Technology is responsible for creating, updating, and implementing this Policy.

5.2 Backup creation and maintenance

The Division of Information Technology will ensure that Backups of Electronic Records are maintained and purged in accordance with this Policy.

5.3 Records hold

A Records Hold is necessary following the initiation or anticipated initiation of governmental or regulatory investigations and administrative or legal proceedings regarding the Archdiocese and/or its officers, directors, agents, or employees. In the event any employee learns of any proceeding or anticipates the initiation of a proceeding, he or she should immediately inform the Division Director, who should then immediately contact the

Director of Information Technology and Archdiocesan Legal Counsel to initiate a Records Hold.

1100.6 Destruction of Backup Storage:

6.1 Periodic Destruction:

Except where a Department/Division formally adopts a longer retention period, all Monthly Backups should be purged in accordance with this Policy.

6.2 Ensuring Litigation Hold is not in Place Prior to Destruction:

The Director of Information Technology is responsible for ensuring that a Monthly Backup is not subject to a Records Hold prior to destruction.

6.3 Three-Year Destruction Schedule:

A Monthly Backup that has been retained for at least three (3) years since its creation should be purged using appropriate electronic data destruction procedures, except that a Monthly Backup for the month of December should not be purged.

6.4 Destroying Existing Monthly Backups:

Any Monthly Backups in existence as of the effective date of this Policy that were created more than three (3) years earlier should be purged using appropriate electronic data destruction procedures, with the caveat that a Monthly Backup for the month of December should not be purged.

6.5 Retained Records:

Absent a Records Hold, ordinary implementation of this Policy should result in the following Monthly Backups being retained: 1) those less than three years old and 2) Monthly Backups for the month of December (regardless of age).

1000 Third-Party Vendor Management Policy v2

October 16, 2024October 27, 2025

1000 THIRD-PARTY VENDOR MANAGEMENT POLICY

1000.1 Purpose:

The purpose of this Third-Party Vendor Management Policy is to establish guidelines and procedures for the selection, engagement, and ongoing management of third-party vendors by the Archdiocese of Baltimore.
This policy ensures that all third-party vendors adhere to the Archdiocese's standards for **security, privacy, and compliance** to safeguard sensitive information and maintain the organization's reputation.

1000.2 Scope:

This policy applies to all **employees, volunteers, contractors, and affiliates** of the Archdiocese of Baltimore who engage with or hold responsibilities related to third-party vendors.

1000.3 Vendor Selection:

1000.3.1 Due Diligence

a. Prior to engaging any third-party vendor, a thorough evaluation shall be conducted to assess qualifications, capabilities, and reliability.
b. The due diligence process must include assessment of the vendor's **security practices, privacy policies, regulatory compliance, financial stability, and reputation**.

1000.3.2 Vendor Evaluation Criteria

a. Vendors must demonstrate a commitment to maintaining the highest standards of **security, privacy, and ethical conduct**.
b. Evaluation criteria may include **experience, references, certifications, security controls, disaster recovery plans, and insurance coverage**.

1000.4 Contractual Requirements:

1000.4.1 Security and Privacy Requirements

a. Contracts with third-party vendors shall include provisions requiring compliance with applicable **security standards, regulations, and data protection laws**.
b. Vendors must agree to protect the **confidentiality, integrity, and availability** of all sensitive information shared with them.

1000.4.2 Data Handling and Processing

a. Vendors must handle and process data in accordance with the Archdiocese's **data protection and privacy policies**.
b. Data sharing, retention, and disposal requirements must be clearly defined within the contract.

1000.4.3 Right to Audit

a. The Archdiocese reserves the right to conduct **periodic audits or assessments** of the vendor's security controls, practices, and compliance.
b. Vendors must cooperate fully with audit requests and provide necessary documentation or evidence upon request.

1000.5 Ongoing Vendor Management:

1000.5.1 Vendor Performance Monitoring

a. Regular performance evaluations shall be conducted to assess the vendor's adherence to contractual obligations and service level agreements (SLAs).

b. Monitoring activities may include reviewing **security incident reports, service quality metrics, and feedback** from internal stakeholders.

1000.5.2 Incident Response and Business Continuity

a. Vendors must maintain **incident response and business continuity plans** to minimize disruption and mitigate risks.
b. Procedures for reporting and managing **security incidents or breaches** must be jointly established between the vendor and the Archdiocese.

1000.6 Use of Third-Party Applications in Microsoft Azure:

1000.6.1 Policy Requirement

Only **Microsoft-certified applications** may be integrated or utilized within the Archdiocese's Microsoft Azure Enterprise environment. Use of non-Microsoft-certified third-party applications is prohibited unless a formal exception is granted per section 1000.6.4.

1000.6.2 Security & Compliance Rationale

a. Microsoft-certified applications undergo **rigorous testing, validation, and ongoing review** to ensure compliance with security, privacy, and reliability standards.
b. Non-certified applications pose risks such as uncontrolled updates, inadequate encryption, hidden vulnerabilities, and regulatory non-compliance.
c. Restricting Azure integrations to certified apps helps maintain governance, reduce the attack surface, and ensure consistency in support and incident response.

1000.6.3 Operational Enforcement

a. All requests to integrate or enable third-party applications in Azure must be submitted to the **IT/Security Team** for review.

b. Only applications listed in Microsoft's official **Certified Azure Enterprise Applications Catalog** shall be approved.
c. Approved applications will be documented and monitored in the organization's **vendor/integration register**.
d. Periodic audits shall confirm continued compliance with certification, security updates, and enterprise alignment.

1000.6.4 Exceptions & Risk Assessment

a. Exceptions may be considered only with **written approval** from the CIO/CTO or Head of IT Security.
b. Exception requests must include a full **security and compliance risk assessment**, including threat modeling, encryption review, and vendor support evaluation.
c. Documented mitigation strategies must be approved and monitored for the duration of the exception.

1000.6.5 Non-Compliance

a. Use of non-certified applications without approval constitutes a **violation** of this policy.
b. Violations may trigger revocation of access, removal of the application, contract review, or disciplinary action per section 1000.9.
c. If a certified application loses certification or becomes deprecated, IT must evaluate alternatives or plan a controlled decommission.

1000.7 Domain Name Registration and Management:

1000.7.1 Policy Requirement

All Archdiocesan **parishes, schools, and affiliated centers** must have their registered internet domain names managed within the Archdiocese's **centralized Cloudflare account**. No entity shall independently register or manage domains outside of this centralized environment.

1000.7.2 Purpose and Rationale

a. Centralized management ensures **security, operational consistency, and business continuity** across all Archdiocesan entities.
b. Cloudflare provides **enterprise-level protection** including DNS security, redundancy, DDoS mitigation, and SSL management.
c. Decentralized or independently managed domains pose significant risks—such as **domain expiration, hijacking, DNS misconfiguration, lack of monitoring, or delayed incident response**.

1000.7.3 Implementation Requirements

a. All new or existing domains must be **registered, transferred, or delegated** into the official Archdiocese Cloudflare account under the Technology Department's management.
b. IT will maintain an **authoritative domain inventory**, documenting ownership, expiration, DNS records, and associated services.
c. Any vendor or hosting provider supporting Archdiocesan domains must coordinate with the Technology Department to ensure compliance.
d. All DNS updates and configuration changes must be performed or approved by **authorized Technology Department staff**.

1000.7.4 Exceptions and Transitional Provisions

a. Legacy domains under separate management must be **reviewed and transitioned** during the next renewal cycle or as otherwise directed.
b. The Technology Department will assist all entities through the migration and validation process.

1000.8 Termination and Transition:

Procedures will be established to ensure a **secure and orderly transition**

and retrieval of all Archdiocese-owned data and assets upon vendor contract termination or expiration.

1000.9 Compliance and Consequences:

Failure to comply with this Third-Party Vendor Management Policy may result in **contract termination, legal action, or disciplinary measures**, depending on the severity and frequency of non-compliance.

1000.10 Policy Review:

This policy will be **periodically reviewed and updated** by the Technology Department to ensure continued alignment with evolving security risks, regulatory requirements, and organizational needs.

900 Employee Training and Awareness Policy v2

October 16, 2024January 11, 2026

900 EMPLOYEE TRAINING AND AWARENESS POLICY

900.1 Purpose:

The purpose of this Employee Training and Awareness Policy is to ensure that all employees of the Archdiocese of Baltimore receive the necessary training and guidance to understand their responsibilities in maintaining a secure and compliant environment. This policy aims to raise awareness of information security best practices, privacy regulations, and ethical conduct in line with the mission and values of the organization.

900.2 Scope:

This policy applies to all employees, volunteers, contractors, and any

individuals affiliated with the Archdiocese of Baltimore who handle, access, or process sensitive information or have responsibilities related to information security.

900.3 Training Program:

3.1. Initial Training

a. All new employees and volunteers will receive comprehensive training on information security policies, procedures, and practices during their onboarding process.

b. The initial training will cover topics such as data protection, acceptable use of technology resources, confidentiality requirements, and compliance with relevant laws and regulations.

3.2. Ongoing Training

a. Regular training sessions will be conducted to reinforce information security awareness and promote a culture of privacy and compliance.

b. Training sessions will cover emerging threats, new technologies, changes in regulations, and any relevant updates to policies and procedures.

900.4 Training Topics:

4.1. Information Security

a. Importance of information security and the potential risks associated with data breaches, cyber threats, and unauthorized disclosure.

b. Best practices for creating strong passwords, securing devices, and protecting sensitive information.

c. Recognizing and reporting security incidents, phishing attempts, and suspicious activities.

4.2. Data Protection and Privacy

a. Understanding the organization’s data protection and privacy policies, including the handling of personal and confidential information.

b. Compliance with applicable data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or other local privacy laws.

4.3. Ethical Conduct

a. Upholding ethical standards in the use of technology. handling of

information, and interactions with colleagues, clients, and stakeholders.
b. Promoting inclusivity, respect, and professionalism in all communication channels, including email, social media, and other online platforms.

900.5 Recordkeeping:

Records of employee training sessions, attendance. and completion will be maintained to track compliance with training requirements.

900.6 Compliance and Consequences:

Failure to comply with the Employee Training and Awareness Policy may result in disciplinary action, up to and including retraining. suspension, or termination of employment or volunteer service, depending on the severity and frequency of the violation.

900.7 Policy Review:

This Employee Training and Awareness Policy will be reviewed periodically to ensure its effectiveness, relevance, and compliance with changing social media trends and legal requirements.

800 Social Media Policy v2

October 14, 2024January 11, 2026

800 SOCIAL MEDIA POLICY

800.1 Purpose:

The purpose of this Social Media Policy is to provide guidelines and standards for the appropriate and responsible use of social media platforms by employees, volunteers, contractors, and any individuals representing the Archdiocese of Baltimore. The policy aims to ensure the organization’s

reputation, protect confidential information, and promote respectful and ethical behavior in the online environment.

800.2 Scope:

This policy applies to all individuals associated with the Archdiocese of Baltimore who utilize social media platforms on behalf of the organization or in com1ection with their roles or responsibilities.

800.3 General Guidelines:

3 .1. Professional Conduct

a. Use social media platfo1ms in a professional manner, upholding the values, teachings, and mission of the Archdiocese of Baltimore.

b. Exercise good judgment and maintain respectful and courteous communication when engaging with others online.

3.2. Personal Responsibility

a. Clearly differentiate personal opinions from official statements or views of the Archdiocese of Baltimore.

b. Take personal responsibility for all content posted on personal social media accounts that may reflect on the organization’s reputation.

3 .3. Privacy and Confidentiality

a. Respect the privacy and confidentiality of individuals and confidential information associated with the Archdiocese of Baltimore.

b. Refrain from disclosing sensitive or confidential information about the organization, its members, donors, or partners without proper authorization.

3.4. Intellectual Property

a. Respect copyright laws and intellectual property rights when sharing content on social media platforms.

b. Obtain proper permissions and give credit to original sources when using or sharing copyrighted materials.

800.4 Representing the Archdiocese of Baltimore:

4.1. Official Social Media Accounts

a. Only authorized individuals should create and manage official social media accounts representing the Archdiocese of Baltimore.
b. Maintain consistency with the organization’s branding. tone. and messaging in all official social media communications.

4.2. Personal Endorsements and Recommendations

a. Clearly indicate personal views as separate from official endorsements or recommendations of the Archdiocese of Baltimore.
b. Exercise caution when associating personal social media profiles with the organization to avoid potential misinterpretation or confusion.

800.5 Reporting Violations:

Any suspected violations of this Social Media Policy should be rep0rted to the designated authority or the Human Resources Department of the Archdiocese of Baltimore.

800.6 Consequences of Policy Violations:

Violation of this Social Media Policy may result in disciplinary action, up to and including termination of employment or volunteer service, depending on the severity and frequency of the violation.

800.7 Policy Review:

This Social Media Policy will be reviewed periodically to ensure its effectiveness, relevance, and compliance with changing social media trends and legal requirements.

700 Disaster Recovery Policy v2

October 14, 2024January 11, 2026

700 DISASTER RECOVERY POLICY

700.1 Purpose:

The purpose of this Disaster Recovery Policy is to establish a framework for the timely recovery and restoration of critical systems, data, and services in the event of a disaster or major disruption at the Archdiocese of Baltimore. The policy aims to ensure the organization's ability to resume essential operations and minimize the impact of disruptions on its mission and stakeholders.

700.2 Scope:

This policy applies to all employees, volunteers, contractors, and any individuals who have access to the Archdiocese of Baltimore's systems, data, and network resources.

700.3 Disaster Recovery Framework:

3.1. Business Impact Analysis (BIA)

a. A comprehensive business impact analysis will be conducted to identify critical systems, applications, and data assets, and determine the maximum allowable downtime and recovery time objectives.

b. The BIA will help prioritize recovery efforts and allocate resources accordingly.

3.2. Disaster Recovery Plan (DRP)

a. A disaster recovery plan will be developed. maintained, and regularly tested to provide guidelines, procedures, and responsibilities for recovering critical systems and services.

b. The DRP will include step-by-step instructions for data backup and restoration, system recovery, communication, and post-recovery activities.

3.3. Data Backup and Recovery

a. Regular backups of critical data and systems will be performed and stored in a secure and off-site location.

b. Backup procedures will be documented and tested to ensure the integrity and availability of backups for recovery purposes.

3.4. Alternative Facilities and Infrastructure

a. Alternative facilities, such as a secondary data center or cloud

infrastructure, will be identified and prepared to facilitate the recovery of critical systems and services.

b. Redundant hardware, networking, and power systems will be implemented to minimize single points of failure.

700.4 Disaster Recovery Procedures:

4. 1. Disaster Declaration and Activation

a. The authority and process for declaring a disaster and activating the disaster recovery plan will be established.

b. Designated personnel will be responsible for initiating the recovery process and coordinating the efforts of the recovery team.

4.2. Recovery Team Roles and Responsibilities

a. A recovery team comprising representatives from relevant depa1tments will be formed and trained to execute the recovery plan.

b. Roles and responsibilities of recovery team members will be clearly defined to ensure an organized and coordinated response.

4.3 Recovery Process and Testing

a. Recovery procedures, including system restoration. data recovery, and post-recovery validation, will be documented and tested periodically.

b. Regular testing and drills will be conducted to evaluate the effectiveness of the disaster recovery plan and identify areas for improvement.

700.5 Communication and Notification:

a. Clear communication channels will be established to notify relevant stakeholders, including senior management, employees. and external parties. about the disaster and recovery progress.

b. Communication plans will be developed to ensure timely and accurate updates are provided during the recovery process.

700.6 Policy Review:

This Disaster Recovery Policy will be reviewed on a periodic basis to ensure its effectiveness, relevance, and alignment with evolving business needs and industry best practices.

Please note that this is a general example and should be customized to fit the specific needs and requirements of the Catholic organization. It is recommended to seek legal advice and consult with relevant stakeholders when drafting or implementing a Disaster Recovery Policy.

600 Incident Response Policy v2

October 14, 2024January 11, 2026

600 INCIDENT RESPONSE POLICY

600.1 Purpose:

The purpose of this Incident Response Policy is to establish a structured and coordinated approach to detecting, responding to, and recovering from security incidents within the Archdiocese of Baltimore. The policy aims to minimize the impact of incidents, protect sensitive information, and ensure the continuity of operations.

600.2 Scope:

This policy applies to all employees, volunteers, contractors, and any individuals who have access to the Archdiocese of Baltimore's systems, data. and network resources.

600.3 Incident Response Framework:

3.1. Incident Identification

a. Employees and stakeholders are encouraged to promptly report any suspicious activities, security breaches, or potential incidents to the IT department or designated incident response team.

b. Proactive monitoring systems will be implemented to detect and identify potential security incidents.

3.2. Incident Response Team

a. An incident response team comprising representatives from relevant departments will be established to oversee incident response activities.

b. The incident response team will include members with technical expertise, legal knowledge, and communication skills necessary to effectively respond to incidents.

3 .3. Incident Response Plan

a. An incident response plan will be developed, maintained, and regularly reviewed to outline the organization's procedures, roles, and responsibilities during incident response.

b. The incident response plan will address incident assessment, containment, eradication, recovery, and lessons learned.

3 .4. Incident Classification and Escalation

a. Incidents will be classified based on severity impact, and potential risks to the organization.

b. An escalation process will be established to ensure appropriate stakeholders are notified based on the severity and nature of the incident.

600.4 Incident Response Procedures:

4.1. Incident Assessment and Containment

a. The incident response team will promptly assess the nature, scope, and impact of the incident.

b. Immediate actions will be taken to contain and isolate the incident to prevent fu1ther damage and unauthorized access.

4.2. Incident Eradication and Recovery

a. Efforts will be made to eradicate the incident, remove any malicious presence, and restore affected systems to a secure state.

b. Data backups and restoration procedures will be implemented to ensure business continuity and minimize data loss.

4.3. Communication and Reporting

a. Clear communication channels will be established to notify relevant stakeholders, including senior management, legal authorities, and affected individuals, as required by applicable laws and regulations.

b. Incident reports will be generated, documenting the incident details. response actions, and lessons learned.

600.5 Training and Awareness:

a. Ongoing training and awareness programs will be conducted to educate employees about their roles and responsibilities in incident repo1ting and response.
b. Employees will be trained on recognizing potential security incidents, repotting procedures, and incident response best practices.

600.6 Policy Review:

This Incident Response Policy will be reviewed on a periodic basis to ensure its effectiveness and alignment with evolving security threats and industry best practices.
Please note that this is a general example and should be customized to fit the specific needs and requirements of the Catholic organization. It is recommended to seek legal advice and consult with relevant stakeholders when drafting or implementing an Incident Response Policy.

500 Password Policy v2

October 14, 2024January 11, 2026

500 PASSWORD POLICY

500.1 Introduction:

The purpose of this Password Policy is to establish guidelines for creating strong, secure, and confidential passwords to protect the Archdiocese of Baltimore’s systems, data, and network resources from unauthorized access and potential security breaches.

500.2 Purpose:

This policy applies to all employees, volunteers. contractors. and any

individuals who have access to the Archdiocese of Baltimore's systems, data, and network resources.

500.3 Password Creation Guidelines:

3. 1. Complexity Requirements

a. Password Length: Passwords must be a minimum of 8 characters in length.

b. Complexity: Passwords must include a combination of upper and lowercase letters, numbers, and special characters.

c. Avoid Common Patterns: Passwords should not contain common patterns, such as" 12345678″ or "password."

d. Avoid Personal Information: Passwords should not include personal information such as names, birthdays, or addresses.

3.2. Password Management

a. Unique Passwords: Each user must have a unique password for their individual accounts. Password reuse across multiple systems or accounts is strictly prohibited.

b. Regular Password Changes: Users must change their passwords at least every 90 days. Passwords should not be reused within a 12-month period.

c. Restricted Sharing: Passwords must not be shared with others or stored in an insecure manner, such as writing them down or storing them in plain text files.

d. Password Reset: If a password is forgotten or compromised, users must follow the organization's password reset procedures to regain access to their accounts.

500.4 Password Protection:

4.1. Password Storage: Passwords should be stored securely using industry-standard encryption methods. Plaintext storage of passwords is strictly prohibited.

4.2. Account Lockouts: After a certain number of failed login attempts, user accounts will be temporarily locked to prevent unauthorized access. Users must follow the organization's account unlocking procedures to regain access.

4.3. Two-Factor Authentication (2FA): Two-Factor Authentication is strongly recommended for all accounts where technically feasible. It adds an extra layer of security by requiring users to provide additional authentication factors along with their passwords.

500.5 Employee Responsibilities:

5.1. Password Confidentiality: Users must keep their passwords confidential and not share them with anyone, including TT staff or supervisors.

5.2. Reporting Suspicious Activity: Users must promptly report any suspected unauthorized access or suspicious activity related to their passwords or accounts to the IT department or designated IT security contact.

500.6 Compliance and Enforcement:

6.1 . Compliance Monitoring: The Archdiocese of Baltimore reserves the right to monitor password usage and enforce compliance with this policy.

6.2. Consequences of Non-Compliance: Failure to comply with this Password Policy may result in disciplinary actions, including account suspension. loss of access privileges, and potential legal consequences.

500.7 Policy Review:

This Password Policy will be reviewed on a periodic basis to ensure its effectiveness and compliance with evolving security standards and best practices.

Please note that this is a general example and should be customized to fit the specific needs and requirements of the Catholic organization. It is recommended to seek legal advice and consult with relevant stakeholders when drafting or implementing a Password Policy.

500 Password Policy v2

October 13, 2024

500 PASSWORD POLICY

500.1 Introduction:

The purpose of this Password Policy is to establish guidelines for creating strong, secure, and confidential passwords to protect the Archdiocese of Baltimore’s systems, data, and network resources from unauthorized access and potential security breaches.

500.2 Scope:

This policy applies to all employees, volunteers. contractors. and any individuals who have access to the Archdiocese of Baltimore’s systems, data, and network resources.

500.3 Password Creation Guidelines:

3. 1. Complexity Requirements

a. Password Length: Passwords must be a minimum of 8 characters in length.

b. Complexity: Passwords must include a combination of upper and lowercase letters, numbers, and special characters.

c. Avoid Common Patterns: Passwords should not contain common patterns, such as” 12345678″ or “password.”

d. A void Personal Inf01mation: Passwords should not include personal information such as names, birthdays, or addresses.

3.2. Password Management

a. Unique Passwords: Each user must have a unique password for their individual accounts. Password reuse across multiple systems or accounts is strictly prohibited.

b. Regular Password Changes: Users must change their passwords at least every 90 days. Passwords should not be reused within a 12-month period.

c. Restricted Sharing: Passwords must not be shared with others or stored in an insecure maimer, such as writing them down or storing them in plain

text files.

d. Password Reset: If a password is forgotten or compromised, users must follow the Archdiocese of Baltimore's password reset procedures to regain access to their accounts.

500.4 Password Protection:

4.1. Password Storage: Passwords should be stored securely using industry-standard encryption methods. Plaintext storage of passwords is strictly prohibited.

4.2. Account Lockouts: After a certain number of failed login attempts, user accounts will be temporarily locked to prevent unauthorized access. Users must follow the organization's account unlocking procedures to regain access.

4.3. Two-Factor Authentication (2FA): Two-Factor Authentication is strongly recommended for all accounts where technically feasible. It adds an extra layer of security by requiring users to provide additional authentication factors along with their passwords.

500.5 Employee Responsibilities:

5.1. Password Confidentiality: Users must keep their passwords confidential and not share them with anyone, including TT staff or supervisors.

5.2. Reporting Suspicious Activity: Users must promptly report any suspected unauthorized access or suspicious activity related to their passwords or accounts to the IT department or designated IT security contact.

500.6 Compliance and Enforcement:

6.1 . Compliance Monitoring: [Catholic Organization Name] reserves the right to monitor password usage and enforce compliance with this policy.

6.2. Consequences of Non-Compliance: Failure to comply with this Password Policy may result in disciplinary actions, including account suspension. loss of access privileges, and potential legal consequences.

500.7 Policy Review:

This Password Policy will be reviewed on a periodic basis to ensure its effectiveness and compliance with evolving security standards and best practices.

Please note that this is a general example and should be customized to fit the specific needs and requirements of the Catholic organization. It is recommended to seek legal advice and consult with relevant stakeholders when drafting or implementing a Password Policy.

400 Bring Your Own Device (BYOD) Policy v2

October 13, 2024January 11, 2026

400 BRING YOUR OWN DEVICE (BYOD) POLICY

400.1 Introduction:

This Bring Your Own Device (BYOD) Policy outlines the guidelines and responsibilities for employees, volunteers, contractors, and any individuals who use their personal devices to access the Archdiocese of Baltimore’s network, systems, and data. This policy aims to balance the benefits of BYOD with the need to protect sensitive information and maintain a secure computing environment.

400.2 Purpose:

The purpose of this policy is to establish clear expectations and requirements for the use of personal devices in a maimer that ensures the security, confidentiality, and integrity of the Archdiocese of Baltimore’s data. It also aims to provide guidelines for the protection of personal devices from potential security threats.

400.3 Scope:

This policy applies to all individuals who choose to use their personal devices (including but not limited to smartphones, tablets, laptops) to access the Archdiocese of Baltimore's resources, whether on-premises or remotely.

400.4 Policy Guidelines:

4.1 . Device Eligibility: Only devices that meet minimum security requirements and are approved by the IT department may be used for BYOD purposes. The IT department will provide a list of supported devices and operating systems.

4.2. Security Measures: Individuals using personal devices for work-related purposes must ensure the following security measures are implemented:

a. Device Passcode: Devices must be protected with a strong passcode or biometric authentication.

b. Operating System Updates: Devices must have the latest security patches and updates installed.

c. Antivirus and Anti-malware Software: Devices must have up-to-date antivirus and antimalware software installed and regularly updated.

d. Data Encryption: Devices must have data encryption enabled to protect sensitive information in case of loss or theft.

4.3. Access and Authentication: individuals must follow the organization's access and authentication policies when using their personal devices to access the Archdiocese of Baltimore's network or systems. This includes the use of strong, unique passwords, multi-factor authentication where available, and regular password changes.

4.4. Acceptable Use: Individuals must adhere to the Archdiocese of Baltimore's Acceptable Use Policy when using their personal devices for work-related purposes. This includes refraining from accessing or storing inappropriate, offensive. or unauthorized content on their devices.

4.5. Data Protection: Individuals must take appropriate measures to protect the Archdiocese of Baltimore's data when accessed or stored on their personal devices. This includes avoiding unauthorized sharing of data.

using secure file storage and sharing methods approved by the organization, and promptly reporting any data breaches or incidents.
4.6. Remote Wipe: Individuals must acknowledge that the Archdiocese of Baltimore reserves the right to remotely wipe data from personal devices used for work purposes in case of loss, theft, or unauthorized access.
4.7. Employee Liability: Individuals are solely responsible for the security and maintenance of their personal devices, including any associated costs.

400.5 Support and Compliance:

5. 1. Device Support: The organization's IT department will provide limited support for BYOD devices. focusing on network connectivity, access to authorized resources, and assistance with security configurations.
5.2. Compliance Monitoring : The Archdiocese of Baltimore reserves the right to monitor BYOD devices to ensure compliance with this policy and applicable laws. Individuals should have no expectation of privacy when using their personal devices for work-related purposes.

400.6 Policy Acknowledgement:

By using their personal devices for work-related purposes. individuals acknowledge their understanding and acceptance of this BYOD Policy. Failure to comply with this policy may result in disciplinary actions. including the revocation of BYOD privileges and potential legal consequences.
Please note that this is a general example and should be customized to fit the specific needs and requirements of the Catholic organization. It is recommended to seek legal advice and consult with relevant stakeholders when drafting or implementing a BYOD policy.

300 Data Protection and Privacy Policy v2

October 13, 2024January 11, 2026

300 DATA PROTECTION AND PRIVACY POLICY

300.1 Introduction:

This Data Protection and Privacy Policy outlines the principles and guidelines for the collection, use, storage, and protection of personal data within the Archdiocese of Baltimore. This policy applies to all employees, volunteers, contractors, and any individuals involved in processing personal data on behalf of the organization.

300.2 Purpose:

The purpose of this policy is to ensure that personal data is handled in compliance with applicable data protection laws and regulations, including but not limited to the General Data Protection Regulation (GDPR) and other relevant privacy laws. By adhering to this policy, we aim to safeguard individuals' privacy rights, maintain the confidentiality of personal data, and foster trust with our stakeholders.

300.3 Personal Data Collection and Use:

3. 1. Lawful Basis: Personal data will only be collected and processed when there is a lawful basis for doing so, such as with the individual's consent, to fulfill a contract, to comply with legal obligations, or for legitimate interests pursued by the organization.

3.2. Data Minimization: Personal data collected will be limited to what is necessary for the intended purpose and will be kept accurate. up to date, and relevant.

3.3. Purpose Limitation: Personal data will only be used for the specific purposes for which it was collected, unless additional consent is obtained or as required by law.

3.4. Sensitive Data: Special categories of personal data, such as religious beliefs, health information, or criminal records. will be processed in accordance with applicable legal requirements and with explicit consent,

unless otherwise permitted by law.

300.4 Data Subject Rights:

4.1. Right to Access: Individuals have the right to request access to their personal data held by the organization and to receive information about how their data is being processed.

4.2. Right to Rectification: Individuals have the right to request the correction of inaccurate or incomplete personal data.

4.3. Right to Erasure: Individuals have the right to request the deletion of their personal data in certain circumstances, such as when the data is no longer necessary or when consent is withdrawn.

4.4. Right to Restriction of Processing: Individuals have the right to request the restriction of processing their personal data under specific circumstances. such as when the accuracy of the data is contested.

4.5. Right to Data Portability: Where technically feasible. individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another data controller.

300.5 Data Security and Confidentiality:

5. 1. Data Protection Measures: Appropriate technical and organizational measures will be implemented to ensure the security and confidentiality of personal data, including access controls, encryption, regular data backups, and staff training.

5.2. Data Breach Response: In the event of a data breach or unauthorized disclosure of personal data, the organization will follow a documented incident response plan to mitigate the impact, notify affected individuals and relevant authorities, and take necessary corrective actions.

300.6 Data Sharing and Third-Party Processing:

6.1. Third-Party Data Processors: When personal data is shared with third-pa11y service providers or processors, appropriate data processing agreements or contracts will be in place to ensure compliance with data

protection requirements.

6.2. International Data Transfers: If personal data is transferred to countries outside the European Economic Area (EEA), appropriate safeguards and mechanisms will be implemented to ensure an adequate level of data protection as required by applicable laws.

300.7 Data Retention:

7.1. Data Retention Periods: Personal data will be retained only for as long as necessary to fulfill the purposes for which it was collected, unless longer retention is required by law or legitimate organizational purposes.

7.2. Data Disposal: Personal data that is no longer needed will be securely and permanently deleted or disposed of in accordance with applicable legal requirements.

300.8 Staff Responsibilities:

8.1. Training and Awareness: Staff members involved in the processing of personal data will receive appropriate training and awareness programs to ensure their understanding of data protection responsibilities and best practices.

8.2. Confidentiality Obligations: All staff members are required to maintain the confidentiality and security of personal data they handle during their employment or engagement with the organization.

300.9 Compliance and Governance:

9.1. Data Protection Officer: Archdiocese of Baltimore will appoint a Data Protection Officer (DPO) or designate a responsible individual to oversee data protection compliance and act as a point of contact for data subjects and supervisory authorities.

9.2. Data Protection Impact Assessments: Where necessary, Archdiocese of Baltimore will conduct Data Protection Impact Assessments (DPIAs) to assess and mitigate privacy risks associated with data processing activities.

9.3. Policy Review and Updates: This policy will be reviewed periodically

to ensure its continued relevance and compliance with evolving data protection laws and best practices.

300.10 Contact Information:

For any inquiries, requests, or concerns related to this Data Protection and Privacy Policy or the organization's data protection practices, please contact the Data Protection Officer at dpo@archbalt.org.

300.11 Policy Acceptance and Adherence:

All individuals associated with the Archdiocese of Baltimore are required to read, understand, and adhere to this Data Protection and Privacy Policy. Failure to comply may result in disciplinary actions, as outlined in the organization's code of conduct or employment agreements.

This Data Protection and Privacy Policy is effective as of January 1, 2026 and supersedes any previous policies or guidelines related to data protection and privacy.

By implementing this policy, Archdiocese of Baltimore aims to demonstrate its commitment to protecting personal data and respecting the privacy rights of individuals.

200 Information Security Policy v2

October 13, 2024October 21, 2024

200 INFORMATION SECURITY POLICY

200.1 Introduction:

This Information Security Policy outlines the guidelines and measures for protecting the confidentiality, integrity, and availability of information assets with in the Archdiocese of Baltimore. This policy applies to all employees, volunteers, contractors, and any individuals granted access to

the organization’s information systems and data.

200.2 Purpose:

The purpose of this policy is to establish a framework for information security management to ensure the secure handling, storage, and transmission of sensitive information. By adhering to this policy, we aim to protect the organization’s reputation, prevent unauthorized access or disclosure, and comply with legal and regulatory requirements.

200.3 Information Classification:

3.1. Classification Levels: Information assets should be classified into appropriate levels (e.g., Public, Internal, Confidential, Highly Confidential) based on their sensitivity, criticality, and potential impact.

3 .2. Handling and Protection: Each classification level requires specific controls and safeguards to ensure proper handling, storage, transmission, and disposal of information assets.

200.4 Access Control:

4.1. User Access Management: Access to information systems, networks, and data should be granted based on the principle of least privilege. Users should only be given access necessary to perform their job responsibilities.

4.2. User Authentication: Strong authentication mechanisms, such as unique usernames and complex passwords, should be implemented to ensure authorized access and protect against unauthorized use.

4.3 . User Account Management: User accounts should be regularly reviewed, and access rights should be promptly modified or revoked upon changes in job roles or termination of employment.

200.5 Data Protection:

5.1. Data Encryption: Confidential and sensitive data, both at rest and in transit, should be encrypted using approved encryption algorithms and protocols.

5.2. Backup and Recovery: Regular backups of critical data should be

performed and tested to ensure data availability in the event of a system failure. data loss, or a security incident.

5.3 . Mobile Device Security: Mobile devices containing sensitive information should be protected with strong passwords, encrypted storage, and remote wipe capabilities. Appropriate security controls should be implemented to mitigate the risks associated with mobile device use.

200.6 Security Awareness and Training:

6.1. Security Awareness: Regular security awareness programs should be conducted to educate employees and other authorized users about their responsibilities. best practices. and emerging threats.

6.2. Training: Employees and authorized users should receive training on specific security topics relevant to their job roles, such as data handling, incident reporting, and incident response procedures.

200.7 Incident Management:

7. I . Incident Reporting: All security incidents and breaches. including suspected or actual unauthorized access, data breaches, or malware infections, must be reported promptly to the designated IT or security personnel.

7.2. Incident Response: An incident response plan should be in place, outlining the steps to be followed in the event of a security incident. The plan should include roles and responsibilities, communication procedures. and procedures for containment, eradication. and recovery.

200.8 Policy Compliance:

8.1 . Compliance Monitoring: Regular monitoring and auditing of systems, networks, and user activities should be conducted to ensure compliance with this policy and detect any violations or security breaches.

8.2. Policy Review: This policy will be reviewed periodically to align with changing technology, emerging threats, and regulatory requirements. Any updates or modifications will be communicated to all employees and authorized users.

100 Acceptable Use Policy v2

October 13, 2024October 21, 2024

100 ACCEPTABLE USE POLICY

100.1 Introduction:

This Acceptable Use Policy (AUP) outlines the guidelines and expectations for the use of technology resources provided by the Archdiocese of Baltimore. All users, including employees, volunteers, contractors, and any individuals granted access to the organization's technology resources, are required to adhere to this policy.

100.2 Purpose:

The purpose of this policy is to ensure the appropriate and responsible use of technological resources, including computers, networks. internet access. email, and other electronic communications systems. By following this policy, we aim to protect the organization's information assets, maintain the integrity of our systems, and promote a respectful and productive technology environment.

100.3 General Guidelines:

3.1. Compliance: Users must comply with all applicable laws, regulations, and policies governing the use of technology resources.

3.2. Authorized Use: Technology resources provided by the organization are to be used for official purposes and activities related to the organization's mission. Personal use should be limited and should not interfere with work responsibilities.

3.3. Access Control: Users are responsible for safeguarding their login credentials and preventing unauthorized access to their accounts or any confidential information.

3.4. Security: Users must not attempt to bypass security measures, install

unauthorized software, or engage in any activity that may compromise the security or integrity of the organization's systems.

3.5. Privacy: Users should respect the privacy of others and refrain from accessing, using, or disclosing any confidential or personal information without proper authorization.

3.6. Intellectual Property: Users must respect intellectual property rights and should not copy, distribute, or use copyrighted material without proper authorization.

100.4 Internet and Email Use:

4.1. Internet Use: Internet access should be used for work-related purposes. Inappropriate websites, including those containing explicit, offensive, or illegal content, should not be accessed.

4.2. Email Use: Email should be used for official communications and should adhere to the organization's Email Policy. Users should exercise caution when opening email attachments or clicking on links from unknown or suspicious sources.

100.5 Social Media and Online Activities:

5.1. Social Media Use: Users should represent the organization professionally and responsibly on social media platforms. Confidential information or sensitive organization matters should not be shared without proper authorization.

5.2. Online Behavior: Users should engage in respectful and ethical online behavior, refraining from engaging in cyberbullying, harassment, or any other form of harmful or malicious activities.

100.6 Consequences of Violations:

Violations of this policy may result in disciplinary action. including but not limited to verbal or written warnings, temporary or permanent loss of technology privileges, and termination of employment or volunteer status. Legal actions may also be pursued if violations involve illegal activities.

100.7 Policy Review and Updates:

This policy will be reviewed periodically and updated as necessary to address emerging technology trends, legal requirements, and organizational needs. Users will be notified of any policy changes, and they are responsible for familiarizing themselves with the current version of the policy.

By using the organization’s technology resources, users acknowledge that they have read, understood, and agree to abide by the terms and conditions outlined in this Acceptable Use Policy.

201 Disposiciones Generales

December 19, 2018January 24, 2019

201 DISPOSICIONES GENERALES

201.1 Propósito:

Esta Política está diseñada para establecer pautas para las copias de seguridad de ciertos registros electrónicos, así como la retención y destrucción de dicha copia de seguridad.

201.2 Alcance:

Esta Política se aplica a los registros electrónicos que se almacenan en los servidores informáticos y que son propiedad y mantenidos por la Arquidiócesis.

201.3 Los Registros Electrónicos son Propiedad Arquidiocesana:

Todos los registros electrónicos generados o recibidos por la Arquidiócesis son propiedad de la Arquidiócesis. Los empleados no tienen ningún derecho

personal o de propiedad sobre los registros, electrónicos o de otro tipo, creados, recibidos o generados en nombre de la Arquidiócesis. De manera similar, ninguna instalación o entidad de almacenamiento pertenecientes a terceros tienen derechos personales o de propiedad sobre registros, electrónicos o de otro tipo, almacenados por la Arquidiócesis en dicha instalación o entidad.

201.4 Preguntas / Implementación:

Las preguntas sobre la aplicabilidad o implementación de esta Política, incluidas las preguntas sobre la retención de cualquier registro específico, deben dirigirse al Director de Tecnologías de la Información.

201.5 Coordinación con otras Políticas:

Esta política debe interpretarse en conformidad con cualquier otra política de retención de registros electrónicos de la Arquidiócesis. Sin embargo, en el caso de un conflicto específico en cuanto a la copia de seguridad de los registros electrónicos, esta Política prevalecerá.

201.6 Definiciones:

Registro Electrónico – Un Registro Electrónico incluye información grabada, independientemente de su medio o característica, que se almacena en un servidor informático que es propiedad y mantenido por la Arquidiócesis.

Retención de Registros – Una Retención de Registros es el cese de la destrucción de cualquier registro que se relacione con el tema de la Retención de Registros.

Copia de Seguridad – Una Copia de Seguridad, o el proceso de copia de seguridad, hace referencia a la copia y el archivo de datos informáticos para su posterior recuperación.

200 Política Sobre Las Copias De Seguridad De Registros Electrónicos

December 19, 2018January 23, 2019

200 POLÍTICA SOBRE LAS COPIAS DE SEGURIDAD DE REGISTROS ELECTRÓNICOS

---

101 Disposiciones Generales

December 19, 2018January 17, 2019

101 DISPOSICIONES GENERALES

101.1 Propósito:

Esta Política proporciona principios para el uso aceptable e inaceptable de Internet.

101.2 Alcance:

Esta política pretende ser ilustrativa del rango de usos aceptables e inaceptables de Internet y no es necesariamente exhaustiva.

101.3 Preguntas e Informes sobre el Uso:

Las preguntas sobre si un uso específico es aceptable o cuando se trate de informar sobre un uso inaceptables deben dirigirse al supervisor del usuario, al Director de División o al Director de las Tecnologías de la Información.

101.4 Revisión de Presuntas Violaciones:

Las presuntas violaciones de esta Política serán revisadas caso por caso por el Director de la División del usuario, el Director de Tecnologías de la Información y Recursos Humanos (donde el empleado estará sujeto a sanciones disciplinarias por la violación).

101.5 Aplicación:

Cualquier empleado que se descubra que ha violado esta política puede estar sujeto a medidas disciplinarias, que pueden incluir el despido.

101.6 Asunción de Riesgo:

El uso de los Servicios de Internet corre por cuenta del usuario. La Arquidiócesis no ofrece garantías, expresas o implícitas, con respecto a la información o software obtenido de los Servicios de Internet y no será responsable de los daños causados por el uso de los Servicios de Internet, incluida la pérdida de datos, demoras o interrupciones del servicio causadas por cualquier acción, omisión, negligencia o error por parte de la Arquidiócesis.

101.7 Declaración de Divulgación sobre el Acceso a los Ordenadores:

Los usuarios que tengan acceso a los Servicios de Internet deberán revisar y firmar la Declaración de Divulgación de Acceso a los Ordenadores (computadoras), disponible aquí.

Archdiocese of Baltimore Policy

November 29, 2018October 3, 2025

503 VPN Use And Security

October 29, 2018January 22, 2019

503 VPN USE AND SECURITY

503.1 Use of ISP:

Employees with an approved VPN shall use their own internet service provider ("ISP") for access to the Archdiocesan network.

Procedure:

A) The user is responsible for paying any fees associated with the user's ISP.

B) A broadband ISP service with 256K speed or greater is recommended.

C) VPN access via America Online or dial-up services is not supported, due to technological and speed limitations.

503.2 Automatic Disconnections:

The Archdiocesan network will automatically disconnect VPN users after thirty minutes of inactivity. Pings or other artificial network process shall not be used to avoid disconnection.

503.3 Connection Limit:

VPN access may not extend beyond a 24-hour connection limit.

503.4 Expiration of VPN Access:

If a VPN account is not used for a period of six months the account will expire and no longer function.

Procedure:

VPN access is considered an "as needed" privilege, and account activity is monitored. If VPN access expires and is subsequently required, the user must make a new VPN request as described above.

503.5 Unauthorized Users:

Employees with VPN privileges must ensure that unauthorized users are not allowed to access the Archdiocesan network

503.6 Internet Access Prohibited:

To protect the Security of the Archdiocesan network, access to the Internet is strictly prohibited while connected to the VPN. To gain access to the Internet, a user must log out of the VPN connection.

503.7 Compliance with Computer Use and Internet Policy:

VPN users must read and follow the Division of Information Technology's Computer Use and Internet Policy, available here.

502 VPN Eligibility And Requests

October 29, 2018January 31, 2019

502 VPN ELIGIBILITY AND REQUESTS

502.1 Approval for VPN Request:

An employee must obtain approval from the employee's supervisor and Executive Director before submitting a request for VPN Access

502.2 VPN Request Form:

All VPN requests must be made through a VPN Access Request Form, available here .

502.3 Eligibility for VPN:

VPN access will only be granted to exempt employees with an assigned Archdiocesan laptop and whose job functions require VPN access, because:

A) The employee must perform job functions away from the Catholic Center.

B) While performing job functions away from the Catholic Center, the employee requires extensive use of Archdiocesan network applications or of a significant quantity of large network files and/or the need to share such files with other Archdiocesan users.

501 General Provisions

October 29, 2018January 22, 2019

501 GENERAL PROVISIONS

501.1 Scope:

This Policy applies to Virtual Private Network (VPN) use by Catholic Center employees.

501.2 Purpose:

This Policy provides guidelines for Remote Access IPSec or PPTP Virtual Private Network (VPN) connections to the Archdiocesan Network.

501.3 Applicability:

This Policy applies to all archdiocesan employees, contractors, consultants, temporary employees, and other workers using VPNs to access the Archdiocesan network.

501.4 Enforcement:

The Director of Information Technology shall enforce this Policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

403 Other Rules And Restrictions

October 29, 2018January 31, 2019

403 OTHER RULES AND RESTRICTIONS

403.1 Ownership:

All Archdiocesan procured software and hardware, including Smart Phones, are the sole property of the Archdiocese.

403.2 Unapproved Software:

Employees may only install approved software on Archdiocesan Smart Phones.

403.3 Compliance with IT Policies:

Smart Phone users must read and follow the Division of Information Technology's Computer Use and Internet Policy, available here and Mobile Device Security Awareness and Usage Guidelines, available here.

403.4 Password Protection:

Employees must, at a minimum, enable 4-digit password protection within the Smart Phone. It is the sole responsibility of the employee to remember the password. Employees may not disable password protection or enable automatic remembering of passwords.

403.5 Personal Smart Phones:

Employees may not connect their personal Smart Phones to the Archdiocese's computers or network.

403.6 Sensitive Information:

Employees should not store sensitive or confidential Archdiocesan information (including files or documents) on Smart Phones.

403.7 Repairs:

The Division of Information Technology should be contacted if a Smart Phone requires repair. Smart Phones will not be sent for repair until all user/Archdiocesan information is removed.

402 Smart Phone Eligibility And Requests

October 29, 2018January 31, 2019

402 SMART PHONE ELIGIBILITY AND REQUESTS

402.1 Approval for Assignment of Smart Phone:

An employee must obtain approval from the employee's supervisor and Executive Director before submitting a request for assignment of an Archdiocesan owned Smart Phone to the Division of Information Technology.

402.2 Smart Phone Request Form:

All Smart Phone requests must be made through an IT Smart Phone Request Form, available here.

402.3 Eligibility for Assigned Smart Phone:

Eligible employees are exempt employees who often check and respond to email outside of normal working hours, use Microsoft Outlook Calendar to track appointments and schedule meetings and events, and Contacts to store business contact information, and:

1) The employee's job function requires substantial travel outside of the Catholic Center and near instant access to email, contacts, calendars and other Smart Phone functions; or

2) The employee participates in a large quantity of meetings within the Catholic Center which require frequent and immediate coordination with others.

401 General Provisions

October 29, 2018January 22, 2019

401 GENERAL PROVISIONS

401.1 Scope:

This policy applies to Smart Phone use and request for use by Catholic Center employees.

401.2 Purpose:

This policy provides the guidelines for users to request, obtain, and use an Archdiocesan-owned Smart Phone

401.3 Enforcement Authority:

The Director of Information Technology shall enforce this Policy. Any employee found to have violated this policy may be subject to disciplinary

action, up to and including termination of employment.

303 Rules And Restrictions For Laptop Use

October 29, 2018January 31, 2019

303 RULES AND RESTRICTIONS FOR LAPTOP USE

303.1 Ownership:

All Archdiocesan procured computer software and hardware systems and equipment, including laptop computers, are the sole property of the Archdiocese.

303.2 Unapproved Software:

Employees may only install approved software on Archdiocesan laptops.

303.3 Connecting Assigned Laptop to the Network:

Employees with assigned laptops must regularly (at least every 2 weeks) connect to the Archdiocesan network from within the Catholic Center to obtain the latest software updates, including operating system patches and virus updates.

303.4 VPN Connections:

Employees who are assigned laptops are not automatically eligible for Virtual Private Network connections to the Archdiocesan network. Employees seeking this enhanced laptop service must complete a VPN request form in accordance with the VPN Policy, available here.

303.5 Compliance with Computer Use and Internet Policy:

Laptop users must read and follow the Division of Information Technology's

Computer Use and Internet Policy, available here.

303.6 Laptop Security and Usage Guidelines:

Laptop users must read and follow the Division of Information Technology's Laptop Security Awareness and Usage Guidelines, available here.

303.7 Home/Personnel Laptop:

Due to licensing agreement limitations, the Division of Information Technology may not install business software on home/personnel computers (i.e., that are not owned by the Archdiocese).

303.8 Connecting Home/Personnel Laptop to Archdiocesan Network:

Employees may not connect their own personal laptop to the Archdiocesan computer network.

302 Laptop Eligibility Requests

October 29, 2018January 31, 2019

302 LAPTOP ELIGIBILITY AND REQUESTS

302.1 Approval for Assignment of Laptop:

An employee must obtain approval from the employee's supervisor and Executive Director before submitting a request for assignment of a laptop to the Division of Information Technology.

302.2 Laptop Request Form:

All laptop requests must be made through an IT Laptop Request Form, available here.

302.3 Eligibility for Assigned Laptop:

Only employees whose job functions require significant use of computer and/or software products licensed to the Archdiocese while outside of the Catholic Center are eligible to be assigned a laptop computer

302.4 Unassigned Loaner Laptops:

The Archdiocese maintains a pool of “Loaner Laptops” available to meet the needs of employees who require computing outside the Catholic Center on a sporadic, infrequent, or inconsistent basis.

Procedure:

An employee may request a loaner laptop by sending an email request to the Helpdesk (*Helpdesk).

301 General Provisions

October 29, 2018January 22, 2019

301 GENERAL PROVISIONS

301.1 Scope:

This Policy applies to laptop use and requests for use by Catholic Center employees.

301.2 Purpose:

This Policy provides guidelines for users to request, obtain, and use a laptop.

301.3 Procurement:

The Division of Information Technology approves and procures all Archdiocesan hardware and software technology purchases.

301.4 Enforcement:

The Director of Information Technology shall enforce this Policy. Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

203 Destruction Of Backup Storage

October 29, 2018January 22, 2019

203 DESTRUCTION OF BACKUP STORAGE

203.1 Periodic Destruction:

Except where a Department/Division formally adopts a longer retention period, all Monthly Backups should be purged in accordance with this Policy.

203.2 Ensuring Litigation Hold is not in Place Prior to Destruction:

The Director of Information Technology is responsible for ensuring that a Monthly Backup is not subject to a Records Hold prior to destruction.

203.3 Three-Year Destruction Schedule:

A Monthly Backup that has been retained for at least three (3) years since its creation should be purged using appropriate electronic data destruction procedures, except that a Monthly Backup for the month of December should not be purged.

203.4 Destroying Existing Monthly Backups:

Any Monthly Backups in existence as of the effective date of this Policy that were created more than three (3) years earlier should be purged using appropriate electronic data destruction procedures, with the caveat that a Monthly Backup for the month of December should not be purged.

203.5 Retained Records:

Absent a Records Hold, ordinary implementation of this Policy should result in the following Monthly Backups being retained:

1) those less than three years old and

2) Monthly Backups for the month of December (regardless of age).

202 Backup And Retention

October 29, 2018January 22, 2019

202 BACKUP AND RETENTION

202.1 Responsibility for Enforcing and Implementing Policy:

The Director of Information Technology is responsible for creating, updating, and implementing this Policy.

202.2 Creating and Maintaining Backups:

The Division of Information Technology will ensure that Backups of Electronic Records are maintained and purged in accordance with this Policy.

Procedure:

A) Backup of Electronic Records shall occur at the end of each month ("Monthly Backup").

B) A Monthly Backup may be performed and maintained using a method and storage medium selected by the Division of Information Technology (including a medium other than the medium in which an Electronic Record was created).

C) A Monthly Backup should be stored in a secure off-site location.

D) Each Monthly Backup should be retained for at least three (3) years following its creation, with the caveat that a Monthly Backup for the month of December should be retained indefinitely.

202.3 Creating a Records Hold:

A Records Hold is necessary following the initiation or anticipated initiation of governmental or regulatory investigations and administrative or legal proceedings regarding the Archdiocese and/or its officers, directors, agents, or employees. In the event any employee learns of any proceeding or anticipates the initiation of a proceeding, he or she should immediately inform the Division Director, who should then immediately contact the Director of Information Technology and Archdiocesan Legal Counsel to initiate a Records Hold.

201 General Provisions

October 29, 2018January 22, 2019

201 GENERAL PROVISIONS

201.1 Purpose:

This Policy is designed to establish guidelines for backing up certain

electronic records, as well as the retention and destruction of any such backup.

201.2 Scope:

This Policy applies to electronic records that are stored on computer servers owned and maintained by the Archdiocese.

201.3 Electronic Records are Archdiocesan Property:

All electronic records generated or received by the Archdiocese are the property of the Archdiocese. Employees do not have any personal or property rights to records, electronic or otherwise, created, received, or generated on behalf of the Archdiocese. Similarly, no third party storage facility or entity has any personal or property rights to records, electronic or otherwise, stored by the Archdiocese at or with any such facility or entity.

201.4 Questions/Implementation:

Questions about the applicability or implementation of this Policy, including questions about the retention of any specific record, should be directed to the Director of Information Technology.

201.5 Coordination with Other Policies:

This Policy should be interpreted in accordance with any other electronic records retention policy of the Archdiocese. In the event of a specific conflict as to the backup of electronic records, however, this Policy shall control.

201.6 Definitions:

Electronic Record – An Electronic Record includes recorded information, regardless of medium or characteristic, which is stored on a computer server owned and maintained by the Archdiocese.

Records Hold – A Records Hold is the cessation of destruction of any

records that relate to the subject of the Records Hold.

Backup – a Backup, or the process of backing up, refers to the copying and archiving of computer data for later retrieval.

104 Archdiocesan Rights

October 29, 2018January 22, 2019

104 ARCHDIOCESAN RIGHTS

104.1 Right to Access Email Messages and Computer Files:

The Archdiocese reserves the right to access and review all electronic mail messages and accounts transmitted or maintained on the Archdiocese's Internet Services and any and all computer files stored on Archdiocesan-owned equipment. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC § 2510 et seq.), notice is hereby given that there are NO services provided by this system for sending or receiving private or confidential electronic communications.

104.2 Right to Monitor Network Use:

The Archdiocese reserves the right to monitor and log network use and file server space use by users of the Internet Services (users are responsible for complying with all file server space allotments).

104.3 Right to Remove User:

The Archdiocese reserves the right to remove any user's account access to the Internet Services.

104.4 Right to Change Policy:

The Archdiocese reserves the right to change its Computer Use and

Internet Policy (and any other policies related to its Internet Services) at any time.

103 Unacceptable Uses

October 29, 2018January 22, 2019

103 UNACCEPTABLE USES

103.1 Unacceptable Uses Forbidden:

Users shall not use Internet Services for activities unrelated to the mission of the Archdiocese, which includes the following unacceptable uses.

103.2 Illegal Purposes or Activities:

Users shall not use Internet Services for any illegal purpose. The Archdiocese will report any illegal use of the Internet Services to law enforcement authorities (including any messages relating to or in support of illegal activities).

103.3 Inappropriate Materials:

Users shall not use the Internet Services to transmit, receive, or access any threatening, libelous, defamatory, sexual, obscene, or harassing materials or correspondence.

103.4 Unauthorized Distribution:

Users shall not use Internet Services for the unauthorized distribution or publication of Archdiocesan data or information (in particular any proprietary or confidential information).

103.5 Private Purposes:

Users shall not use the Internet Services for personal gain or private purposes unrelated to their Archdiocesan duties, whether for-profit or not, such as private advertising or marketing activities.

103.6 Political Causes:

Users shall not use the Internet Services in support of political causes.

103.7 Consistency with Catholic Religious Beliefs:

Users shall not use the Internet Services to advocate religious beliefs or practices contrary to Roman Catholic teaching or doctrine.

103.8 Representing Private Opinions as those of the Archdiocese:

Users of Internet Services shall not represent that their personal opinions or views represent those of the Archdiocese, and must ensure that no actions or inactions by users cause third-parties to be confused regarding whether an opinion is that of the Archdiocese.

103.9 Virus Protection:

Users shall not use the Internet Services to download software or electronic files without reasonable virus protection measures in place.

103.10 Interference with Operations:

Users shall not use the Internet Services to interfere with or disrupt other users, services, or equipment, or to interfere with the normal operation of any Archdiocesan Internet Services.

101 General Provisions

October 29, 2018September 25, 2024

101 GENERAL PROVISIONS

101.1 Purpose:

More Information

No Content

This Policy provides principles for acceptable and unacceptable use of the internet.

101.2 Scope:

More Information

No Content

This Policy is intended to be illustrative of the range of acceptable and unacceptable uses of the internet and is not necessarily exhaustive.

101.3 Questions and Reports Regarding Use:

More Information

No Content

Questions about whether a specific use is acceptable and reports of unacceptable use should be directed to the user's supervisor, Division Director, or the Director of Information Technology.

101.4 Review of Alleged Violations:

Alleged violations of this Policy will be reviewed on a case-by-case basis by the user's Division Director, the Director of Information Technology, and

Human Resources (where the employee is subject to discipline for the violation).

101.5 Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

101.6 Assumption of Risk:

Use of the Internet Services is at the user's risk. The Archdiocese makes no warranties, express or implied, with regard to information or software obtained from the Internet Services and will not be responsible for any damages caused by use of the Internet Services, including any loss of data, delays, or service interruptions caused by any actions, omissions, negligence, or errors by the Archdiocese.

101.7 Computer Access Disclosure Statement:

Users given access to the Internet Services shall review and sign the Computer Access Disclosure Statement, available here.

100 Computer Use And Internet Policy

October 29, 2018January 22, 2019

100 COMPUTER USE AND INTERNET POLICY

The Internet is an important resource for the Archdiocese to provide better, cheaper, and faster services. The Archdiocese will creatively use the Internet to improve services and contribute broadly to the mission of the Church. The connection to the Internet and related services, communication channels, and computing tools provided by the Archdiocese (the "Internet Services") exist to facilitate the official work of the Archdiocese.The Internet Services are provided for employees and

authorized persons affiliated with the Archdiocese for the efficient exchange of information and the completion of assigned responsibilities consistent with the mission of the Archdiocese. The use of the Internet Services by any employee or other person authorized by the Archdiocese (the "Users") must be consistent with this Policy (including all security and confidentiality provisions set forth herein) and any other Archdiocesan conduct policy, including the Code of Conduct and Harassment policy.

600 Information Privacy Statement

May 30, 2018January 22, 2019

600 INFORMATION PRIVACY STATEMENT

The Archdiocese of Baltimore is committed to maintaining the confidentiality and security of personally identifiable information that it collects, uses and discloses in furtherance of the mission of the Church.

Personal information is kept confidential and used only for the purposes for which it was collected or similar purposes in furtherance of the mission of the Church. The information will not be sold or disclosed for commercial purposes. Aggregate statistical data may be disclosed without individual identifiers for research and reporting purposes.

Reasonable physical, electronic, and procedural safeguards are maintained to protect personal information from unauthorized access, loss, misuse, disclosure, or alteration. Access is restricted to employees or agents of the Archdiocese who require the information in connection with the services they provide.

Individual privacy concerns should first be addressed with the individual's pastor, school principal, human resources manager, or division/department/agency director. If the issue cannot be resolved, an inquiry may be made in writing to the Director of the Division of Information Technology for the Archdiocese of Baltimore.

If you believe that any of the information held by the Archdiocese is incomplete or inaccurate, you have the right to requests updates or corrections. To do so, please contact the Archdiocese of Baltimore Division of Information Technology, 320 Cathedral Street, Baltimore, MD 21201 at 410-547- 5305.

From time to time, this statement may be reviewed to ensure that it remains relevant and appropriate. To obtain a copy of this and other privacy related information, visit https://dev-policy-archdiocese-of-baltimore.pantheonsite.io/privacy.