_TEST_Pages_

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, 2018June 12, 2019

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, 2018November 24, 2022

101 GENERAL PROVISIONS

101.1 Purpose:

More Information

What is Lorem Ipsum?

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

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

101.2 Scope:

More Information

What is Lorem Ipsum?

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem

Ipsum.

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

What is Lorem Ipsum?

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

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.