

# **ARCHDIOCESE OF WASHINGTON**

## **CENTRAL PASTORAL ADMINISTRATION**

This policy is not yet promulgated in the parishes, but includes prudent guidance that parishes can choose to implement.



## **INFORMATION TECHNOLOGY SECURITY POLICY**



DONALD CARDINAL WUERL  
BY THE GRACE OF GOD AND THE APOSTOLIC SEE  
ARCHBISHOP OF WASHINGTON

## DECREE

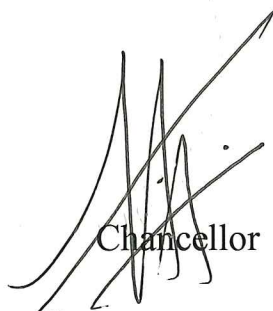
To all who work at the Central Pastoral Administration of the Archdiocese of Washington:

It is my pleasure to approve and promulgate the Information Technology Security Policy for the Central Pastoral Administration of the Archdiocese of Washington. This policy is designed to publish and enforce the standards and expectations involved in operating the most secure computing environment possible for the archdiocese.

This policy is the foundation of the IT security program for the Central Pastoral Administration. Adhering to this policy will enhance the archdiocese's established culture of transparency, trust and integrity. This policy is in place to protect employees, volunteers, partners and the archdiocese itself from exposing information systems or confidential data to individuals who could use access in an unlawful or damaging manner. Also, it is designed to prevent archdiocesan IT assets from being used in an inappropriate way to the detriment of the archdiocese or any individual.

This Information Technology Security Policy for the Central Pastoral Administration is effective immediately and replaces any prior policies and guidelines concerning information technology security for the Central Pastoral Administration.

Given this fourteenth day of February, two thousand and seventeen in the Archdiocese of Washington.



Chancellor



Archbishop of Washington



# ARCHDIOCESE OF WASHINGTON

Archdiocesan Pastoral Center: 5001 Eastern Avenue, Hyattsville, MD 20782-3447  
Mailing Address: Post Office Box 29260, Washington, DC 20017-0260  
301-853-4500

Vicar General  
and Moderator of the Curia

February 14, 2017

Dear Colleagues,

It is a pleasure to present the recently promulgated Information Technology (IT) Security Policy for the Central Pastoral Administration of the Archdiocese of Washington. This policy will enforce and inform users and secretariats of the archdiocese of the standards and expectations involved in operating the most secure and practical computing environment possible. The scope of the policy includes, but is not limited to, the operation and procurement of physical computers, as well as the use of the network, software, and applications.

In publishing and distributing the IT Security Policy, the intent of archdiocesan management and the Archdiocesan IT Office is to enhance our established culture of transparency, trust, and integrity. These policies and procedures are in place to protect employees, volunteers, partners, and the Archdiocese of Washington from either knowingly or unknowingly exposing information systems or confidential data to individuals who could use access in an unlawful or damaging manner and to also prevent archdiocesan IT assets from being inappropriately used.

The IT Security Policy was approved by the Archbishop of Washington on February 14, 2017 and became effective immediately. It is my hope that this policy will better protect the Information Technology Infrastructure and Data assets of the Central Pastoral Administration. Please contact Mr. Will Potter, CIO and Executive Director of Information Technology ([potterw@adw.org](mailto:potterw@adw.org) or 301-853-4494), with any questions you may have.

With kind regards, I am

Sincerely in Christ,

Most Reverend Barry C. Knestout  
Vicar General and Moderator of the Curia



**ARCHDIOCESE OF WASHINGTON**

DEPARTMENT OF INFORMATION TECHNOLOGY

(301) 853-4444

**ARCHDIOCESE OF WASHINGTON**  
**CENTRAL PASTORAL ADMINISTRATION**  
**INFORMATION TECHNOLOGY SECURITY POLICY**  
**2017**

<b>Version</b>	1.9
<b>Last Updated</b>	1/22/2017

## List of Acronyms & Abbreviations

<b>Acronym</b>	<b>Meaning</b>
----------------	----------------

ADW	Archdiocese of Washington
-----	---------------------------

EDI	Electronic Data Interchange
-----	-----------------------------

FTP	File Transfer Protocol
-----	------------------------

IT	Information Technology
----	------------------------

PEM	Privacy Enhanced Mail
-----	-----------------------

## Contact Information

ADW Finance and Management  
Chief Financial Officer

Eric Simontis  
Extension 365

ADW Information Technology (IT) CIO & Executive Director

Will Potter  
Extension 494

ADW Information Technology (IT)  
[it@adw.org](mailto:it@adw.org) (CPA)

Tech Support  
Extension 444  
Telephone #: 301-853-4444

# Contents

Acronym ii

Meaning ii

## **Contact Information..... ii**

## **1. Introduction..... 1**

## **2. Overview ..... 1**

## **3. Purpose and Scope ..... 1**

## **4. ADW Technology and Information Assets ..... 1**

### 4.1. Physical Assets ..... 1

#### 4.1.1. Personal Use of Physical Assets..... 1

#### 4.1.2. Mobile Device Management ..... 3

### 4.2. Information Assets ..... 4

#### 4.2.1. Defining ADW Information Assets ..... 4

#### 4.2.2. Securing Information Assets..... 4

#### 4.2.3. Transporting and Transmitting Information Assets ..... 4

#### 4.2.4. Unauthorized Use of ADW Information Assets ..... 4

### 4.3. Third Party Information Assets ..... 5

#### 4.3.1. Confidentiality Agreement for Third Parties..... 5

#### 4.3.2. Management of Third Party Services..... 6

#### 4.3.3. Third Party Access ..... 6

### 4.4. Use of Physical and Information Assets ..... 7

#### 4.4.1. Use for Business Purposes..... 7

#### 4.4.2. Personal Use..... 7

#### 4.4.3. Restrictions of Use ..... 7

#### 4.4.4. Prohibited Use ..... 8

#### 4.4.5. Consequences for Inappropriate or Prohibited Use..... 8

## **5. Network Security..... 8**

### 5.1. Network Password Complexity ..... 8

#### 5.1.1. Reference ADW User Level Password Policy..... 8

### 5.2. Securing Your Workstation..... 8

#### 5.2.1. Locking Your Workstation..... 8

#### 5.2.2. Logging Off Your Workstation ..... 8

### 5.3. Securing Your Data ..... 8

#### 5.3.1. Save Files on Network Drives ..... 8

#### 5.3.2. Removable Media ..... 8

#### 5.3.3. Laptop Devices..... 9

#### 5.3.4. FTP Services ..... 9

#### 5.3.5. Secure FTP and Secure File Share Services ..... 9

#### 5.3.6. Personal Cloud Services..... 9

### 5.4. Reporting Security Problems ..... 9

#### 5.4.1. Incident Notification (Potential Security Violation)..... 9

#### 5.4.2. Unauthorized Access and Disclosure of Information ..... 9

#### 5.4.3. Notification of Unauthorized Use..... 9

#### 5.4.4. Unauthorized Network Information Gathering ..... 10

### 5.5. Approved Network Devices ..... 10

#### 5.5.1. Connecting to internal networks ..... 10

### 5.6. Network Changes and External Access ..... 10

## **6. Keeping Email Safe and Secure ..... 10**

### 6.1. Prohibited Use..... 10

### 6.2. Email Security Best Practices..... 11

#### 6.2.1. Validating Email Addresses ..... 11

#### 6.2.2. Emailing Confidential or Sensitive Data..... 11

#### 6.2.3. Emailing Information to Personal Accounts..... 11

#### 6.2.4. HIPAA Regulations and Email ..... 11

#### 6.2.5. Email Confidentiality Signature..... 11

### 6.3. Email Attachments..... 12

6.4.	Message Forwarding .....	12
6.5.	Bulk Mailings .....	12
6.6.	Bulk Mail Best Practices .....	12
6.7.	Retention of Email.....	12
6.8.	Remote Access to Email.....	13
<b>7.</b>	<b>Viruses, Spyware, and Other Malicious Software.....</b>	<b>13</b>
<b>8.</b>	<b>Web Browsing .....</b>	<b>13</b>
8.1.	Internet Content Filtering .....	13
8.2.	No Expectation of Privacy .....	14
8.3.	Public Representations on the Internet .....	14
8.3.1.	ADW Affiliation .....	14
8.3.2.	External Representations on Behalf of ADW .....	14
8.3.3.	Internal ADW Disclosure .....	14
8.4.	Bandwidth Usage.....	14
8.5.	Social Networking .....	14
<b>9.</b>	<b>Privacy .....</b>	<b>15</b>
9.1.	ADW Privacy Statement.....	15
<b>10.</b>	<b>Computer Software.....</b>	<b>15</b>
10.1.	Required Consultation with the IT Office.....	15
10.2.	Downloading and Installing Software.....	15
10.3.	Licensed Software.....	15
<b>11.</b>	<b>Policy Violations .....</b>	<b>16</b>
<b>12.</b>	<b>Responsibilities and Best Practices .....</b>	<b>16</b>
12.1.	Information Technology (IT) Staff.....	16
12.1.1.	Policies and Technical Guidance.....	16
12.1.2.	Compliance Monitoring .....	16
12.1.3.	Risk Mitigation.....	16
12.1.4.	Security Measures .....	16
12.1.5.	User Access Controls.....	16
12.1.6.	Application and Service Rollout.....	16
12.1.7.	Tech Support.....	16
12.2.	Professional Service Providers .....	17
<b>Summary</b>	<b>.....</b>	<b>18</b>
<b>Glossary</b>	<b>.....</b>	<b>19</b>
<b>Acknowledgement of Receipt.....</b>		<b>25</b>
<b>To Report a Security Concern .....</b>		<b>26</b>

---

## 1. Introduction

This document is designed to enforce and inform users and secretariats of the Archdiocese of Washington of the standards and expectations involved in operating the most secure computing environment possible and that is most practical for ADW. The scope of this policy transcends aspects of the entire organization. It includes, but is not limited to, both the operation and procurement of physical computers, the network and its infrastructure, as well as use of software and applications.

## 2. Overview

The Information Technology Security Policy is the foundation of the IT security program for ADW. In publishing and distributing this security policy, the intent of ADW management and the ADW IT office is to enhance ADW's established culture of transparency, trust and integrity. These policies and procedures are in place to protect employees, volunteers, partners and ADW itself from either knowingly or unknowingly exposing information systems or confidential data to individuals who could use access in an unlawful or damaging manner, and also to prevent ADW IT assets from being used in an inappropriate way to the detriment of ADW or any individual.

Effective security is a team effort involving the participation and support of **everyone** who deals with ADW information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly. This policy will be reviewed annually and updated based on changes as dictated by security standards.

## 3. Purpose and Scope

The purpose of this policy is to establish management direction, procedures and requirements as they relate to information security. This policy applies to all employees, clergy, contractors, consultants, temporary workers, volunteers, guests and other users of ADW information technology, including those users affiliated with third parties who access ADW computer networks (hereinafter referenced as *users*). The policy also applies to all computer and data communication systems owned by and/or administered by ADW.

All *users* are expected to be familiar with and comply with these policies.

## 4. ADW Technology and Information Assets

### 4.1. Physical Assets

#### 4.1.1. Personal Use of Physical Assets

All IT assets are to be used for ADW business purposes only. Prior approval by the secretaries and executive directors is required for personal use of an ADW computer or ADW asset (e.g., projector, camcorder, and digital camera). This section further describes the acceptable use of ADW computer equipment and applies to all users of information technology within the ADW. In general, employees are responsible for exercising good judgment regarding reasonable personal use.

#### *Physical security*

- Employees are required to safeguard all ADW equipment assigned to their exclusive or shared use, and all ADW equipment within their work area.
- Employees traveling with laptop computers will always carry them in carry-on baggage and not in checked baggage.

---

### *Information security*

- Data created on ADW systems remains ADW's property. The organization cannot guarantee the confidentiality of information stored on any network device.
- All laptops will have encryption setup as additional security method to protect data when laptops are out of the CPA
- For security and network maintenance purposes, individuals authorized by the IT Manager may monitor equipment, systems, and network traffic at any time.
- Secure all idle PCs, laptops, and workstations by forcing password re-entry after a period of time.

### *Self-help*

All users of ADW equipment are expected to take charge of their own training:

- Attend breakfast with IT and/or other in-house classes provided by the IT department.
- Review and become familiar with software documentation.

### *Unacceptable use*

The Diocese/Parish has taken the necessary actions to assure the safety and security of our network. Any individual who attempts to disable, defeat or circumvent security measures is subject to disciplinary action up to and including dismissal. The following are examples of actions and activities that are prohibited: They generally fall into one of three categories confidentiality, security, or illegality. Although many of them overlap into multiple categories

#### Confidentiality

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the diocese/parish/school, or use of classified government information.
2. Using or attempting to use administrative accounts or other network accounts without authorization
3. Stealing, using or disclosing another user's password or credential without authorization.
4. Providing information about, or lists of, staff, students, or parishioners to parties outside the diocese/parish/school.
5. Use of peer-to-peer file sharing software to access, share or trade any files.

#### Illegality

1. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted video, and the installation of any copyrighted software for which the diocese/parish/school or the end user does not have a valid, active license is strictly prohibited.
2. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal and prohibited.
3. Using any network systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, Canon Law, or Diocesan rules and policies. This includes morally objectionable materials, files, images, text or other content

- 
4. Any use of computer equipment that violates state or U.S. law and regulations
  5. Using ADW equipment for personal profit, political fundraising, gambling activity, non-business-related instant messaging or chat room discussions, and downloading or display of offensive material.

## Security

1. Knowingly or negligently introducing viruses, Trojans, worms, or other commands, scripts or programs intended to damage, disable, or degrade computer systems or network resources or to make unauthorized access of networks or systems.
2. Defeating or attempting to defeat content filtering systems.
3. Security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
4. Port scanning, intrusion detection or other security scanning is expressly prohibited by anyone other than systems administrators charged with responsibility for system security.
5. Executing any form of network monitoring which will intercept data not intended for the employee's system, unless this activity is a part of the employee's normal job/duty.
6. Circumventing user authentication or security of any host, system, network or account, or disguising or attempting to disguise the identity of a host, system, account, or service on the network.
7. Interfering with or denying service to any other user (for example, denial of service attack).
8. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable network systems by any means, locally or via the network.
9. Use of resources which are wasteful or which monopolize system resources at the expense of other users.
10. Employees are never authorized to disable the anti-virus software on their workstation.
11. Attempting to compromise systems and databases or acting to disrupt systems or cause unnecessary network congestion or application delays.
12. Use of remote control software on any internal or external host personal computers or systems not specifically set up by the IT staff.

### 4.1.2. Mobile Device Management

ADW IT Department reserves the right to create, manage and enforce security policy for all mobile devices that contain ADW data, including but not limited to iPhones, iPads, laptops and other mobile equipment. The policy for Mobile Device Management is currently under development.

#### Use of Physical Assets Outside of ADW Facilities

Anyone who uses ADW physical assets, including but not limited to laptops and portable storage media, outside of ADW facilities, must:

1. Ensure the asset is secured or under your control at all times, particularly when not in use.
2. Keep ADW data only on ADW IT assets. Do not store ADW data on your home computer or other devices.
3. Use the same security practices when using a device at home as you do in the office – lock your laptop when you step away even for a moment; keep your password secret; and ensure any confidential or potentially sensitive information is protected.

---

## **4.2. Information Assets**

### **4.2.1. Defining ADW Information Assets**

All information traveling over ADW computer and telephone networks, or stored on ADW systems that has not been specifically identified as the property of other parties, either by trademark or copyright, will be treated as an ADW information asset. ADW data contained within hosted, “cloud”, or software as a service (SaaS) services is also considered an ADW information asset. This would include any data stored in CHRIS, ParishSOFT and other mission critical services.

### **4.2.2. Securing Information Assets**

- Files containing confidential or sensitive data should be placed in restricted folders limited only to those users who need access.
- Shared network locations should only permit access to those members of staff that require it.
- In all systems and applications, operate on a principle of least privilege, allowing only permission that is strictly necessary for the business need.
- Restricted folders on the various ADW drives should be used for securely sharing files between program locations or departments requiring access.
  - Submit a Help Desk ticket to request a restricted folder on any shared drive.
- When printing sensitive data, use the private print feature on the multi-function devices. (Contact help desk for assistance)
- To ensure confidentiality, secure any hardcopies of confidential or sensitive data in a locked file cabinet or desk drawer.
- Shred hardcopies containing confidential or sensitive data when you are finished using them in accordance with ADW Records Retention and Document Destruction protocols and policies.

### **4.2.3. Transporting and Transmitting Information Assets**

- Personally Identifiable Information (PII), Health Insurance Portability and Accountability Act (HIPAA), or other data sensitive in nature is not to be transmitted in non-secure formats or through insecure communication methods.
- With required approvals, sensitive data should be transmitted via an approved secure transfer method. Transporting sensitive data outside of ADW facilities in any other form is prohibited. If transmitted over insecure medium such as email or Dropbox, files must at minimum be encrypted or otherwise securely packaged.
- Sensitive information must not be displayed, uploaded or transmitted using web conference software (WebEx, GoToMeeting or Skype for example). If web conference attendees require access to sensitive information, transmit it separately via an approved method, following all rules and requirements for such transmissions.
- When conducting a video teleconference, ensure that any sensitive information is out of the viewing range of the camera.
- If non-sensitive ADW data must leave the program site, it should be accessed on an ADW laptop or mobile device through secure Virtual Private Network (VPN) or Citrix access, or on a secure USB device.

### **4.2.4. Unauthorized Use of ADW Information Assets**

The unauthorized access, disclosure, duplication, modification, transfer, diversion, destruction, loss, misuse or theft of sensitive or confidential data is strictly prohibited and may result in disciplinary action or termination.

---

### 4.3. Third Party Information Assets

It is the policy of ADW to protect information belonging to third parties that has been entrusted to ADW in confidence, as well as in accordance with applicable contracts and industry standards.

This section sets forth security requirements to be observed by all employees who are responsible for managing relationships with third parties throughout the organization.

#### 4.3.1. Confidentiality Agreement for Third Parties

Where there is a business need to disclose any sensitive information of ADW to third parties (such as business partners and contractors), or grant third parties access to sensitive information, the management of ADW must execute a confidentiality agreement or an agreement that incorporates confidentiality provisions with such third parties in advance. This Third Party confidentiality agreement is different than the employee confidentiality agreement.

It is prohibited for the employees of ADW to disclose sensitive information to a third party or to grant a third party access to sensitive information, without execution of a confidentiality or similar agreement.

#### Requirements of the Confidentiality Agreement

Security requirements must be identified and incorporated in the confidentiality or similar agreement, based on the confidentiality of the information.

The following requirements shall be incorporated in the confidentiality or similar agreement as fundamental obligations of the third party that has possession of ADW sensitive information.

- A. It shall strictly keep in confidence and not disclose or disseminate to any other party the sensitive information and shall not use the sensitive information without ADW prior written consent for any purpose other than those stipulated in the confidentiality or similar agreement. (Third parties' obligations of confidentiality shall be perpetual as to the confidential information for which any laws/regulations provide specific requirements, such as personal information).
- B. In order to protect sensitive information, the recipient shall undertake the following:
  - 1. Not to make any copy or reproduction of the sensitive information without ADW prior consent (exceptions may be required, such as in the case of authorized external lawyers using ADW materials);
  - 2. To use the same degree of care in protecting the confidentiality of the sensitive information as the receiving party would use to protect its own confidential and proprietary information of a similar nature (but in any event, no less than a reasonable degree of care, or as required by law), to avoid disclosure, publication or dissemination of the information, including all derivative materials that the receiving party would produce or make during the course of the usage of the sensitive information; and

- 
3. Without limiting any of the foregoing obligations: i) to use a secure method (e.g., encryption) when transmitting sensitive information; ii) to ensure that ADW sensitive information is not commingled with any other organization's confidential information and iii) to notify ADW of any suspected, potential or actual breach of security or other exposure involving sensitive information.

C. If requested by ADW, the recipient shall promptly return or destroy all sensitive information in its possession in a secure manner and shall provide ADW with a declaration to that effect in a form satisfactory to ADW, duly executed.

D. The recipient shall permit personnel designated by ADW to review the recipient's security procedures for the protection of sensitive information at least annually (during normal business hours or otherwise at such parties' consent). At ADW option, such review may include, without limitation, performing penetration testing and vulnerability scans, observing operations, reviewing documents and other materials, and interviewing relevant personnel of the recipient. If, upon such review, ADW determines that the recipient is not in compliance with the terms agreed, ADW shall so notify the recipient in writing of such non-compliance. In the event of such non-compliance, ADW shall have the right to terminate its agreement with the recipient and to take other actions and seek such remedies as appropriate under the circumstances.

#### **4.3.2. Management of Third Party Services**

##### *Third-Party Qualifications*

All potential third-party service agreements that include the disclosure of or access to sensitive information as described in the Confidentiality Agreement must include the Confidentiality Agreement requirements outlined in this policy.

Depending on individual circumstances, the business unit may choose to review the information security practices of the third party. Sample checklists and questionnaires are provided in the appendices as one means of conducting this review.

##### *Service Agreement*

The employee responsible for managing the third party must define specific procedures to ensure that, before work starts, a service agreement is defined and executed, and that it conforms to the security standards of ADW in accordance with legal and regulatory requirements.

##### *Observation of ADW Rules*

Where the services are performed at ADW premises, the employee responsible for managing the third party must have the third party service providers observe and agree to comply with rules related to information security while on ADW premises, and obtain from them a written undertaking to observe the rules adopted for the relevant ADW premises.

#### **4.3.3. Third Party Access**

Access to sensitive information on ADW premises must only be granted to third parties in controlled circumstances and must be approved with clear reference to the reason why access is necessary. These reasons include approved on-site

---

maintenance or where specialist support is required with access to systems and/or premises. Examples of on-site third parties include

- Hardware and software maintenance and support staff;
- Cleaning, catering, security guards and other outsourced support services;
- Student placement and other casual short-term appointments; or
- Consultants.

#### *External Connectivity Process*

In a case where there is a requirement to connect the network of a third party with ADW network, business and technical reasons for requiring such a connection must be documented and a full risk assessment must be completed and approved by ADW IT Department or appropriate delegated authority, and the documentation and the approved risk assessment must be retained for audit purposes.

### **4.4. Use of Physical and Information Assets**

The use of ADW resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

#### **4.4.1. Use for Business Purposes**

All ADW systems, including but not limited to computer equipment, telephone equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing and other network services are the property of ADW. These systems are intended for business purposes in serving the interests of ADW, of our parishioners, pastors and the Church in the course of normal operations

#### **4.4.2. Personal Use**

ADW electronic communications systems are generally restricted to legitimate business activities. Incidental personal use on non-work time is permissible so long as:

- It is not an excessive drain on IT resources, such as network bandwidth (amount of data transmitted) or network storage capacity.
- It does not interfere with staff productivity.
- It does not preempt any ADW activity.
- It is approved by the user's secretaries and executive directors.

Nothing contained in this policy, any other ADW policy, or in the users' access and/or use of these ADW systems is intended to convey personal ownership or any expectation of privacy in the use of these ADW systems.

#### **4.4.3. Restrictions of Use**

Diocesan policy against sexual or other harassment applies fully to ADW communication assets. ADW communication assets must not be used to create or transmit messages that may constitute intimidating, hostile or offensive material on the basis of gender, race, color, religion, national origin, disability or any other protected classification.

Any use of ADW communications assets for abusive, threatening, obscene, insulting, or otherwise inappropriate speech or conduct is strictly forbidden and may result in the employee's termination. Just as ADW prohibits employees from

---

possessing pornographic, sexually offensive, or other inappropriate or offensive materials on Archdiocesan property or at work-related events, ADW also prohibits users from sending, receiving, storing or viewing pornographic, sexually offensive or other inappropriate or offensive material of any kind using ADW communication assets. Any gambling or casino related activity is also prohibited on all ADW computer assets.

#### **4.4.4. Prohibited Use**

Users are prohibited from utilizing ADW physical or information assets to participate in any criminal activity or other activities in direct contradiction of Church teachings. Additionally, excessive personal use is prohibited, as is any activity resulting in personal financial gain.

#### **4.4.5. Consequences for Inappropriate or Prohibited Use**

Users found to have violated sections 4.4.3 (Restrictions of Use) or 4.4.4. (Prohibited Use) may also be deemed to have violated ADW Employment Policies including Policies 260-61, 810, 830-33, and/or 921. Violations of the aforementioned Employment Policies may result in disciplinary action, up to and including immediate termination of employment.

## **5. Network Security**

### **5.1. Network Password Complexity**

#### **5.1.1. Reference ADW User Level Password Policy**

#### **5.1.2. Reference ADW Admin Level Password Policy**

### **5.2. Securing Your Workstation**

#### **5.2.1. Locking Your Workstation**

Users **MUST** secure their workstation when they will be away from their work area however, workstations are configured to automatically lock upon fifteen minutes of inactivity. Upon returning, you will need to enter your password to unlock the workstation.

#### **5.2.2. Logging Off Your Workstation**

Alternatively, a user may choose to log off their workstation when away. This is the recommended procedure especially, when you will be away from your workstation for an extended period of time, or when using your computer off-site.

### **5.3. Securing Your Data**

#### **5.3.1. Save Files on Network Drives**

Save all files on network drives (i.e. G, H, or J drives), rather than on the local hard drive (i.e. C drive), to ensure that they will be backed up by the IT office. The IT office highly discourages users from saving files to the local computer. Files saved to the local computer are saved to the local hard drive and are not backed up.

#### **5.3.2. Removable Media**

Use of unsecured or personal external storage for transportation of ADW data is not permitted. All ADW workstations and laptops have Endpoint Protection installed, which will not allow non-ADW portable storage devices to be plugged in to ADW assets. The IT department will be issuing memory sticks for ADW usage.

---

Authorization from the IT Department will be required for the use of non-ADW removable media (e.g. CDs, flash drives, jump drives, keychain drives, etc.) as they will be blocked by default

### **5.3.3. Laptop Devices**

ADW users should **never** store confidential or sensitive data on laptop devices. Sensitive information must be stored in an approved, centralized, secure and backed up location. All ADW laptops are to have full disk encryption to alleviate concerns with loss or theft.

### **5.3.4. FTP Services**

Users must not place ADW material (files, documents, software, etc.) on any computer that supports unsecure anonymous file transfer protocol (FTP) or similar services; unless the user has permission from ADW management and has requested an IT review and approval of the FTP, application and computer on which they intend to post the materials.

### **5.3.5. Secure FTP and Secure File Share Services**

ADW IT will shortly be creating a process for securely transmitting data outside the ADW network. This process will allow users to securely send and receive data to and from outside entities, to password protect documents, and to set an expiration date for documents so they can only be accessed for a limited duration.

- Details of this process will be contained in a subsequent version of this document.

### **5.3.6. Personal Cloud Services**

Cloud storage services – such as Dropbox, Box, Google Docs, Microsoft OneDrive, and others – are prohibited for the storage and transmission of ADW data. For document and file sharing within ADW, use network shares or SharePoint. For out-of-network access or with external users, please use the approved file sharing services and tools. For more information, contact the Help Desk.

## **5.4. Reporting Security Problems**

To report a real or potential security concern, immediately call the Help Desk at 301-853-4444 or ext.444 or e-mail at [it@adw.org](mailto:it@adw.org).

### **5.4.1. Incident Notification (Potential Security Violation)**

If confidential or sensitive ADW information is lost, compromised, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the user must notify the IT executive director and ADW management immediately (see instructions above). We are required, by law, to notify individuals whose information may have been compromised.

### **5.4.2. Unauthorized Access and Disclosure of Information**

Unauthorized access to information by a user, whether intentional or unintentional, requires that the IT executive director or security & system administrator be notified immediately of the access via a Help Desk ticket submission. The user is not to disclose such information to other parties and must maintain its confidentiality.

### **5.4.3. Notification of Unauthorized Use**

If any unauthorized use of ADW's information systems has taken place, or is suspected of taking place, ADW management and the IT executive director or security & system administrator must be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, disclosed, or suspected of being lost, stolen or disclosed, ADW Management and the IT executive director or security & system administrator must be notified immediately Reporting Unusual System Behavior

---

Because it may indicate a computer virus infection or a similar security problem, all unusual systems behavior (e.g., missing files, frequent system crashes, misrouted messages) must be immediately reported to IT by calling the Help Desk at 301-853-4444 or ext.444.

The specifics of security problems may only be discussed and shared on a need-to-know basis.

#### 5.4.4. Unauthorized Network Information Gathering

Users are not permitted to run network or other system scanning tools to gather data about network or computer equipment. Use of such tools can interrupt and impede network performance and reliability.

### 5.5. Approved Network Devices

For security and administrative reasons, ADW does not permit internal access to personal or outside (non-ADW) devices on any ADW network. This includes, but is not limited to, mobile phones, tablets, laptop/notebook computers, and portable gaming devices. The network is a Microsoft Windows Server environment with only approved Microsoft Windows devices (laptops or desktops) being able to connect.

Approved filtered internet access on guest (insecure) wireless networks is in place as a convenience only for guests, personal employee devices; or other non-ADW domain managed devices

#### 5.5.1. Connecting to internal networks

ADW domain managed devices will connect automatically to internal wireless networks via 802.1x authentication. Similarly, ADW domain managed devices will be granted full access on wired networks.

### 5.6. Network Changes and External Access

Users may not establish internet or other external network connections that could allow non-ADW users to gain access to ADW systems and information. That is to say only ADW equipment can connect to the ADW network. A change request must be submitted and vetted through the IT department to request firewall or other network configuration changes for your application or particular need.

## 6. Keeping Email Safe and Secure

ADW encourages all employees to communicate on business matters using voice mail, email, etc. to enhance productivity and efficiency. All messages generated on or handled by these forms of equipment are ADW property and are not the property of users of the electronic communications services. ADW email addresses should be used for all ADW correspondence. **Do not use personal email accounts to transmit ADW business communications.** Users have no expectation of privacy in such communications (see section 9 below.)

### 6.1. Prohibited Use

ADW communication systems, including email, shall not to be used for the creation or distribution of any disruptive or offensive messages; Please refer back to section 4.4.3 for further details on other types of prohibited uses. Employees who receive any emails with this content from any ADW employee should report the matter to their supervisor immediately.

---

## 6.2. Email Security Best Practices

### 6.2.1. Validating Email Addresses

Contacts made over the Internet should not be trusted with ADW information unless the validity of the source has been verified. This due diligence process applies to the release of any internal ADW information.

### 6.2.2. Emailing Confidential or Sensitive Data

ADW e-mail communications are not guaranteed to be automatically encrypted or protected, and should not be used in the transmission of sensitive data. Please see section 4.2 (Information Assets) for more information regarding transmitting sensitive information. Please contact the Help Desk for more information or assistance.

### 6.2.3. Emailing Information to Personal Accounts

Employees are prohibited from using a personal email account for any ADW business correspondence. If an employee needs to access any ADW data off-site, upon authorization of the user's activity by his/her secretaries and executive directors, the IT office can assist in instructing the user how to access that data through secure means.

If it is determined that an employee has sent confidential or sensitive data to their personal email account without the prior knowledge and permission of their Secretaries and Executive Directors, the employee will be subject to disciplinary action up to and including termination.

### 6.2.4. HIPAA Regulations and Email

ADW is required to comply with regulations of The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA information is divided into two main categories

- PHI = Protected Health Information (refers to information about someone's health – medical, dental and vision plan)
- PII = Personally Identifiable Information (refers to information that can be used to uniquely identify, contact, or locate an individual, or can be used with other sources to uniquely identify a person - social security number, DOB, passport number, etc.)

It is not permitted to email PHI and PII information unless the data is contained within an encrypted email, or sent using an approved file sharing tool.

PII data should ONLY be stored in approved restricted network locations and not on any portable devices or local computers.

Unencrypted emails should not include PHI. Do not forward email messages that contain PHI. Instead, prepare a new message without PHI.

PHI information should be stored in approved network locations, in specially designated ADW applications, and not on any portable devices, media or local computers. If any portable media contains PII or PHI data, this media should be securely wiped or destroyed. If you need assistance, contact IT Help Desk.

### 6.2.5. Email Confidentiality Signature

Emails leaving the ADW network will contain the following disclaimer or something similar, "The information contained in this communication from <user>@ADW.org sent at <Date and Time> is confidential and may be legally privileged. It is intended solely for use by the intended recipient and others authorized to receive it. If you have received this communication in error, you are hereby notified that any disclosure, copying, distribution or taking action in reliance of the contents of this information is strictly prohibited and may be unlawful."

---

### 6.3. Email Attachments

Users are expected to exercise caution when opening email attachments. Do not open email attachments if they are unexpected or suspicious in nature. Users may receive email viruses that appear to come from a familiar source, so it is important to refrain from clicking on attachments that are unexpected. IT has the authority to block email messages that may contain attachments that may be harmful to the network, in accord with current industry practices, and may limit the size of email attachments as necessary.

- Email messages greater than 30MB will not be delivered. Contact the IT Help Desk to send or receive larger files.
- Contact the IT Help Desk if you have questions about our spam filter, bounced messages, mass mailings, or other email transit related issues.

### 6.4. Message Forwarding

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding or replying-all to messages. ADW sensitive information must not be forwarded to any party outside ADW without the prior approval of secretaries and executive directors or ADW management. Blanket forwarding of messages to parties outside ADW is prohibited unless the prior permission of the IT executive director has been obtained.

Permanent forwarding of ADW email addresses or mailboxes to external personal or non-ADW accounts is prohibited.

### 6.5. Bulk Mailings

Mass mailings of greater than 300 recipients out of the ADW network are not permitted. For mass mailings of greater than 300 recipients, an external bulk mailing service is to be used. Please contact the Help Desk in this instance. This prevents performance and mail queue issues locally, and preserves the reputation of our network address space on the internet as legitimate senders.

### 6.6. Bulk Mail Best Practices

When using the Contact lists located in the Outlook Global Address Book for group mailings, it is mandatory that the group email address(es) be inserted in the “BCC” (blind carbon copy) field, rather than the “To” field. This will protect the privacy of the individuals whose addresses are contained in the contact list, as well as eliminate unintentional email traffic when “Reply All” is accidentally selected. It is good practice in general to do this with any group mailing.

### 6.7. Retention of Email

Auto archiving is used centrally to archive email that is older than two years. Nothing needs to be done by the user as this is done automatically. For litigation and records retention policy needs, data should not be deleted.

All incoming and outgoing email, to both internal and external senders is to be retained in a separate mailbox database for the purposes of legal discovery.

---

## 6.8. Remote Access to Email

Remote access to ADW desktop or laptop computers using the Internet is prohibited unless approved by ADW management and the IT executive director. Users, however, are allowed to access email from home or on an approved device by using Outlook Web App. If you have an ADW laptop, you may use a VPN client to log in to the network remotely.

To access email remotely, go to  
<https://outlook.adw.org/owa> (for Outlook Web App)

Instructions for connecting through Outlook Web App are available from the IT Help Desk.

## 7. Viruses, Spyware, and Other Malicious Software

Malicious Code is defined as all software that has been deliberately designed to harm or abuse the resources of computing systems. It is frequently concealed within, or masquerades as, legitimate software.

Malicious Code includes, but is not limited to, viruses, Trojan horses, worms, logic bombs, file infectors, malicious macros, malicious scripts (e.g. Java, ActiveX), malicious cookies, key loggers, and hidden software for launching denial-of-service attacks. Malicious software is designed to take full or partial control of your computer or damage your computer or data without your informed consent. These steps are recommended to prevent problems with malicious software:

- All ADW workstations and laptops have Trend Micro Endpoint antivirus software installed
- Do not click on pop-up ads.
- Never open any files or Microsoft Office document macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately.
- Never download files from unknown or suspicious sources.
- Do not click on links that are unknown or suspicious; especially email links.
- Delete spam, chain, and other junk email. Do not forward chain messages or similar messages to other users.
- Delete suspect security notifications or messages. Do not click on any links in the messages.
- Do not connect ADW removable media to public or shared computers outside of ADW without the explicit permission of the IT office. Non-ADW computers may be infected with malware and that could be transmitted to the removable media device.

## 8. Web Browsing

Internet connectivity presents the organization with new risks that must be addressed in order to safeguard ADW's vital information assets and sensitive data. All users must follow the practices outlined in this document and exercise good judgement when browsing websites.

---

### 8.1. Internet Content Filtering

ADW requires centralized content filtering software to help prevent users from intentionally or unintentionally reaching either inappropriate or unsafe web sites. This activity is to be centrally logged and can be accessed by managers upon request. Logging aside, these types of web content filters are strictly necessary in an environment today where so many threats are web-based.

---

## **8.2. No Expectation of Privacy**

Users of ADW information systems and/or the internet should remember that their communications are not automatically protected from viewing by third parties, unless encryption or other security measures are used, users should not send information they consider private over insecure channels on the Internet.

Nothing contained in this policy, any other ADW policy, or in the users' access and/or use of the ADW information systems is intended to convey any expectation of privacy in the use of the ADW systems.

## **8.3. Public Representations on the Internet**

Some ADW jobs may require professional participation in social media. Users in these jobs have permission to post appropriate job-related messages on these sites using only their ADW email address or affiliated account. All postings related to the user's work with ADW must be cleared with one's supervisor prior to being placed on social media.

### **8.3.1. ADW Affiliation**

All other employees are prohibited from participating in social media using any ADW affiliated account, including personal ADW email, because readers of such postings might mistakenly view an employee's personal statement as expressing the opinion of ADW potentially leading to loss of reputation and/or legal ramifications.

### **8.3.2. External Representations on Behalf of ADW**

All external representations on behalf of ADW must be approved by and is the responsibility of the Communications Secretariat. Any social media posting by a user with his/her ADW email address is considered an external representation under this policy.

### **8.3.3. Internal ADW Disclosure**

Staff must not publicly disclose internal ADW information via the Internet unless the approval of ADW management has first been obtained. This includes information about ADW policies, procedures or other internal confidential information not meant for public release.

## **8.4. Bandwidth Usage**

Users are expected to be considerate in their use of shared internet and network resources. The IT department reserves the right at any time to alter the types of services and content accessible on the ADW network to ensure the reliability and performance of network links.

## **8.5. Social Networking**

Contact the IT office for guidelines before beginning any social networking initiatives for your program or office. Program social networking profiles must be approved by the Communications Secretariat and must have multiple employees administering the account. Individual social network accounts or profiles must not be used in place of organizational accounts. All material contained on these accounts must be in line with Church teachings and ADW guidelines.

New technologies or social networking sites may not be introduced without the prior approval of the Communications Secretariat. Please contact Communications Secretariat for more information.

---

## **9. Privacy**

### **9.1. ADW Privacy Statement**

All information and messages that are created, sent, received or stored using ADW communication assets are the sole property of ADW and no user has any ownership interest or expectation of privacy in such communications. ADW retains the right, in its sole discretion, to review all information or communications sent, received, stored, or posted using ADW communication assets. ADW also retains the right to track internet usage and file downloads for compliance with this policy and for other business reasons. ADW has the right to conduct such review without prior notice to the user. By availing him/herself of the information systems, the user consents to IT and ADW management personnel to grant access to and review of all materials created, stored, sent or received, by the user through any ADW network or internet connection. This includes any information or email accessed by any personal device. Users may not intercept or disclose, or assist in intercepting or disclosing, electronic communications.

ADW management and the IT staff will not review the content of an individual user's communications out of personal curiosity or at the request of individuals who have not gone through the proper approval process.

A program director must file a request to the ADW Executive Director of Human Resources to have email messages or internet activity reviewed or monitored. The Executive Director of Human Resources will authorize or deny monitoring based on the circumstances provided in the request. If authorized, the Executive Director of Human Resources will contact the IT executive director to initiate the review/monitoring. The results will be returned to the Executive Director of Human Resources.

## **10. Computer Software**

IT is responsible for all on-premises workstation, server, network, application and other computer-related assets. Any addition, removal or change to computer related assets must go through the IT department.

### **10.1. Required Consultation with the IT Office**

ADW Management and IT must be consulted prior to seeking advice from outside IT consultants or purchasing any computer-related items or services. This is necessary to ensure that new hardware, software or services can be supported and can safely integrate into the current operating environment.

### **10.2. Downloading and Installing Software**

Only the IT Department and designated third parties are permitted to install or update software on ADW computers. Any requests for new software or updated versions of existing software should be made to the IT Department. Uncontrolled software installations may result in configurations which affect the security, integrity, and stability of the networks (e.g., due to interactions with other software), do not allow for standardization of inventory and maintenance procedures, and increase the labor needed to maintain and overhaul systems.

### **10.3. Licensed Software**

In keeping with the licensing agreements, all ADW software, documentation, and other types of internal information must not be sold or otherwise transferred to any non-ADW party for any non-work related purposes unless expressly authorized by ADW management.

---

## 11. Policy Violations

Violation of these policies may subject users to disciplinary actions, up to and including termination. Questions about this policy may be directed to the Executive Director of Information Technology.

## 12. Responsibilities and Best Practices

As defined below, ADW groups and staff members responsible for communications security have been designated in order to establish a clear line of authority and responsibility in addition to the responsibilities outlined in the previous sections of this policy.

### 12.1. Information Technology (IT) Staff

The IT staff is responsible for maintaining on-premises IT assets.

#### 12.1.1. Policies and Technical Guidance

IT staff establishes email and internet security policies and standards and provides technical guidance on security to all ADW staff.

#### 12.1.2. Compliance Monitoring

IT staff monitors compliance with regulations and provides administrative support for computer and network security requirements, including hardware, software, email, internet security and data safeguards. This includes all installed applications. Third-party hosted applications or SaaS applications are maintained by the service providers.

#### 12.1.3. Risk Mitigation

IT staff monitors each of the critical applications and servers for which they are responsible to find any vulnerabilities and mitigate them as appropriate. On an ongoing basis, any available security patches or updates are to be applied as appropriate as part of this process.

#### 12.1.4. Security Measures

IT staff checks to ensure that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity. IT staff also keeps all servers and applications for which they are responsible up date to with the most current security patches. IT staff also follows up on security incident reports.

#### 12.1.5. User Access Controls

Users' access to network drives and critical applications are reviewed on an annual basis by IT along with the department heads. IT staff ensures that user access controls are defined on these systems in a manner consistent with their duties and information needs. If a staff member leaves employment at ADW, a process is in place to eliminate their access.

#### 12.1.6. Application and Service Rollout

Any new service or application, regardless of whether it is hosted on premise or in a hosted, or "cloud", environment is to be fully reviewed and approved by the IT Department as part of the selection process. Departments should contact the IT Department for assistance in reviewing vendors and products. Unapproved products will not be supported by the Help Desk, and may be blocked from use.

#### 12.1.7. Tech Support

IT staff constantly monitors Help Desk requests during normal business hours, Monday through Friday 8:30 am to 5:00 pm.

---

Secretaries and Executive Directors ensure that users under their supervision comply with the network security policy established in this document.

Secretaries and Executive Directors must ensure that:

- Users under their supervision delete sensitive and confidential data when the data is no longer needed or useful.
- Users under their supervision are aware of and comply with the policies and procedures outlined in all ADW documents that address information security, including this policy.
- The Secretaries and Executive Directors should ensure that users under their supervision follow the off-boarding process, complete the exit clearance process, and return to ADW IT any equipment issued to them (including laptops, phones, encrypted flash drives, etc.) upon their official termination of employment or contractual agreement.
- Requests are submitted to the Help Desk for any changes in network or application access required by users under their supervision. This includes both new users and existing users requiring changes in access.

## **12.2. Professional Service Providers**

In the course of its operations, ADW engages consultants and service providers to assist in carrying out ADW's mission and activities. It is the responsibility of the Secretary and /or Executive Director that has contracted the services of any consultant or external service provider, who is being granted access to data or systems, to ensure the following best practices are applied:

- A background check must be provided by the business or conducted by ADW for any consultant that will be granted access to sensitive / confidential data (e.g. social security or credit card data) or ADW's network.
- Any consultant that will be granted access to sensitive / confidential data must sign a confidentiality agreement.
- For any consultant or third party service provider that will be granted access to sensitive /confidential data or ADW's network, the authorizing department must complete an *IT Department Remote Access Form for Consultants*. Annual submission of the form will be required for long-term engagements.
- Any consultant that will be granted access to sensitive /confidential data or ADW's network must receive the ADW's IT Security Policy and agree to adhere to its contents.

## Summary

The Information Technology Security Policy is the foundation of the IT security program for ADW. In publishing and distributing of this security policy, the intent of ADW management and the ADW IT Department is to enhance ADW's established culture of transparency, trust, and integrity. These policies and procedures are in place to protect employees, volunteers, partners, and ADW itself from either knowingly or unknowingly exposing information systems or confidential data to individuals who could use access in an unlawful or damaging manner, and also to prevent ADW IT assets from being used in an inappropriate way to the detriment of ADW or any individual. Furthermore, this document defines policy to protect the over security of the ADW computer assets.

The document is broken down into the following sections or key topics: ADW Technology and Information Assets; Network Security; Keeping Email Safe and Secure; Viruses, Spyware, and Other Malicious Software; Web Browsing; Privacy; Computer Software; Policy Violations; and Responsibilities and Best Practices.

The topic on ADW Technology and Information Assets discusses the physical assets, and information assets of ADW and how or how not to use physical and information assets. This section drives home the fact that assets of the ADW are not just physical assets but the data that is contained on the equipment is also considered an asset.

One of the key topics of the IT security policy is that of network security. Within the policy the following topics were discussed in great deal network password complexity, securing your workstation; securing your data, approved network devices, and network changes and external access. Within the section on network security it is important to note the timeliness of reporting security problems.

Just as important as network security is that of keeping email safe and secure. This document goes into great detail on the subject of email as it has the potential to be a source of risk and vulnerability for the ADW. To help reduce our risk and chances of virus activity this section defined email security best practices as well as defined email prohibited uses. Enough cannot be said on the importance of understanding the vulnerability of email attachments and how they can be a source of viruses entering into the ADW computer environment. The section on email also discusses bulk mailings. Our outlook / exchange email environment is not designed for sending large bulk emailing, the section further defines bulk mail best practices. The policy lays out guidelines for the safe use of remote access to email whether a laptop is used remotely or the user is using a cell phone or tablet. The final part of the section deals with retention of email and how and why this is important.

One of the later parts of the document dealt with the internet, and discusses safe browsing techniques and ways to prevent getting viruses, spyware, and other malicious software attacks. The ADW IT department does various levels of internet and web content filtering. It should be noted because all computer assets are the property of ADW. The use of these computer assets, including the internet is for business use; employees should have no expectation of privacy if they are using these assets for none business use.

The internet capacity has a limit and all users are requested to be mindful of social media and video usage if it is not directly related to business usage.

Those who operate and maintain the computers and network environments have a duty to protect the ADW assets from misuse, as well as to prevent risk and issues from occurring. Many of these risk and/or issues are rooted in security concerns. Effective security is a team effort involving the participation and support of everyone who deals with ADW information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly

# Glossary

## ADW DOMAIN

Active Directory joined ADW computers or devices. Archdiocese of Washington computers or devices that are organized centrally in an environment called an active directory.

## ANTI-VIRUS SOFTWARE

Computer software used to prevent, detect and remove malicious software.

## ASSETS

The hardware (computers, monitors, servers) and software (Word, Excel) used by ADW employees in their daily work.

## BANDWIDTH

The maximum level of bit rate, or data transfer, that can be sustained on a particular network or communications link.

## CITRIX

Terminal server and application virtualization software that allows users to run applications or a desktop over a network.

## CLOUD

Sometimes used as a metaphor for the Internet, the cloud refers to data, software, servers and services not accessed locally on your workstation but in third-party data centers that could be located across the street or around the world.

## CLOUD STORAGE

These are files and folders stored not on your local workstation but kept in a third-party data center.

## CONFIDENTIALITY AGREEMENT

A document mutually agreed to by two or more parties that stipulates certain information which cannot be divulged outside of the entities listed in the document.

## CONTENT FILTERING SOFTWARE

Also known as content control software, this is s software designed to restrict or control the content a reader is authorized to access, especially when used to restrict material delivered over the internet via the web, email or other means.

## DENIAL OF SERVICE ATTACK

A type of attack on a network that is designed to slow network links to a point of being unusable by flooding it with useless traffic.

## DROPBOX

A file-hosting service operated by Dropbox, Inc., headquartered in San Francisco that offers folder/file storage in a cloud environment, personal cloud storage, file synchronization and an application that installs on your workstation to enable you to access your materials.

## ELECTRONIC DATA INTERCHANGE

The electronic exchange of business information using a standardized format. This is a process which allows one entity to send information to another electronically rather than with paper.

## EMAIL CONFIDENTIALITY SIGNATURE

This is additional text typically found at the bottom of an email message, below the sender's signature line, which states that contents of the message are confidential and intended only for the addressee. Standard additional language typically addresses what to do if the message was received in error and how to notify the sender in such cases.

## ENCRYPTION

A method of encoding messages or information in such a way that only authorized persons can read it. Encryption does not prevent a message from being intercepted but denies the message content to an unauthorized interceptor.

## ENDPOINT PROTECTION

Typically, a suite of applications installed on a workstation, laptop or desktop, that may include antivirus, anti-malware protection, disk encryption and firewall features.

## FILE INFECTORS

A type of malware that infects certain files with the intent of causing permanent damage or making them unusable.

## FILE TRANSFER PROTOCOL

A standard network method used to transfer computer files between a workstation or "client" and a server on a computer network. Abbreviated as FTP, this method allows users to upload, download, delete, rename, move and copy files on a server called an "FTP server."

## FLASH DRIVE

Also called "memory sticks" and "thumb drives," a relatively small-capacity, portable storage unit that plugs into the USB port of a desktop computer or laptop.

## FORGED ROUTING

Malicious messages or routing protocols sent to routers or switches that may attempt to impersonate a network path to a malicious destination.

## HIPPA

This is an acronym that stands for the Health Insurance Portability and Accountability Act, a U.S. law designed to provide privacy standards to protect patient medical records and other health information provided to health plans, doctors, hospitals and other health-care providers.

## HOST

Also often referred to as a node it is a broad term to refer to any network-connected device, such as commonly a desktop, server, switch, or firewall.

## INFORMATION ASSETS

Technically, a body of knowledge that is organized and managed as a single entity. For Archdiocese of Washington purposes, this “body” includes all hard-copy and digital files, folders, documents, graphic files, emails and any other piece of information created by employees in the normal course of performing the duties for which they were hired.

## INTELLECTUAL PROPERTY

This refers to creations of the intellect for which a monopoly is assigned by law to the creator. Some examples would be trademarks, copyrighted materials, patents, industrial design rights, trade secrets, and artistic work, including music and literature.

## INTRUSION DETECTION

Use of a device or a software application that monitors a network or systems for known malicious activity, or violations of policy.

## JUMP DRIVE

Alternately referred to as a USB flash drive, data stick, pen drive, memory unit, key chain drive or thumb drive, a jump drive is a portable storage device with a USB connector.

## KEYLOGGERS

A type of surveillance software or spyware that is able to record every keystroke you make to a file, instant message, email and any other information you type at any time using a keyboard.

## KEYCHAIN DRIVE

Alternately referred to as a USB flash drive, data stick, pen drive, memory unit, jump drive or thumb drive, a jump drive is a portable storage device with a USB connector.

## LOGIC BOMBS

A set of instructions secretly incorporated into a program so that if a particular conditions satisfied, the instructions will be carried out, usually with harmful effects.

## MALICIOUS COOKIES

Cookies are text files placed on your computer when you visit a website in order to store certain information which normally does not compromise your privacy. Malicious cookies can also be used to track online activity, supposedly for advertising purposes, and can result in your private data being stolen for malicious purposes.

## MALICIOUS MACROS

An automated process written into a file, such as an Office document, normally used to allow easy replication of tedious tasks. They can be used for nefarious purposes if an attacker distributes a file containing macros with purposefully malicious instructions.

## MALWARE

A class of software that is intended to damage or disable computers and computer systems.

## MB

An abbreviation of megabyte, a unit of digital information equal, approximately, to one million bytes. Other similar units are KB (kilobyte, a unit equal to a thousand bytes), GB (gigabyte, a unit equal to a billion bytes) and TB (terabyte, a unit equal to a million million bytes).

## MOBILE DEVICE MANAGEMENT

This is the administration and management of mobile devices such as smartphones, tablet computers and laptop computers. At the Archdiocese, MDM deals primarily with managing data and email security according to corporate policy.

## MULTI-FUNCTION DEVICES

A device that can do more than one thing, such as a printer that can also make copies, send faxes and scan/deliver documents.

## NETWORK

A broad term for interconnected switches and computers, from the physical cabling, to the underlying IP protocols, to the applications that you run on your computer.

## NETWORK PASSWORD COMPLEXITY

The concept of creating passwords that are difficult to hack. The Archdiocese, for example, has a complex password policy that requires passwords to be a minimum of eight characters long, and include a capital letter, a lower case letter, a number and a special character.

## NETWORK SNIFFING

The act of using computer software or hardware that can intercept and log traffic passing over a digital network.

## PACKET SPOOFING

When transmitted, digital information is broken down into segments of bytes, Packet spoofing is an attempt to present an illegitimate packet as a valid packet from a legitimate source.

## PEER-TO-PEER

The alternative to a client-server relationship, where your computer connects to a server to access information. In a peer to peer relationship, your computer may access another computer just like it, in such a way that they are “equals” to access data or an application.

## PENETRATION TESTING

A broad term for a security test in which data is attempted to be compromised or accessed by an outside “attacker” through various means in an attempt to identify flaws in the security architecture.

## PERSONAL CLOUD SERVICES

Storage and file management services provided by a third-party data center that are personal in nature as opposed to work-related.

## PHI

Protected health information, under U.S. law, is any information about health status, provision of health care, or payment for health care that is created or collected by an individual. Typically, this term is interpreted to mean any part of a patient's medical record or payment history.

## PHYSICAL ASSETS

A physical asset is an item of economic, commercial or exchange value that has a tangible (or material) existence. For the Archdiocese of Washington and for purposes of this security document, computer equipment is a physical asset, including desktop computers, laptop computers, monitors, keyboards, mice, printers, scanners, projectors, multi-functional devices, and the like.

## PII

Personally identifiable information is any data that could potentially identify a specific individual, or distinguish one person from another, so that information thought to be anonymous is no longer so.

## PING FLOODS

A type of denial-of-service.

## PORT SCANNING

An attempt to identify what network ports, where an application may respond or data may be accessed, are open or closed. See "Penetration Testing".

## PORTABLE STORAGE MEDIA

A small hard drive, or a thumb or flash drive, designed to hold any kind of digital data.

## PRIVACY ENHANCED MAIL

An internet standard that provides for secure exchange of electronic mail. PEM uses a range of techniques to allow for confidentiality, sender authentication and message integrity.

## PRIVATE PRINT

A function of printers and multi-functional devices that allows documents sent to a printer to not actually print until the user enters a username and password. This prevents potentially confidential documents from printing when the user is not at the device to retrieve them when they print.

## SCRIPTS

Code written to automate a task or process. Could be written in any number of different languages depending on its application.

## SECURE FILE SHARE SERVICES

A secure network method used to transfer computer files between a workstation or "client" and a server on a computer network. Abbreviated as SFTP, this method allows users to securely upload, download, delete, rename, move and copy files on a server called an "SFTP server."

## SHAREPOINT

Web-based software developed by Microsoft, primarily used as a secure document management or storage solution which can be accessed by authorized users.

## SOCIAL MEDIA

Computer-mediated technologies that allow the creating and sharing of information, ideas, careers interests and other forms of expression via virtual communities and networks.

## SOFTWARE AS A SERVICE

Commonly abbreviated as “SaaS,” a software licensing and delivery model in which the software is licensed to users on a subscription basis and is centrally hosted. These solutions are typically accessed by users via a web browser.

## SPYWARE

Similar to Malware, but often designed more to gather private information as opposed to maliciously destroy data with no regard for contents.

## SYSTEM

Generic term that could refer to a single computer or multiple servers that comprise components of a single application.

## THIRD PARTY ACCESS

Internal network, application, or server access by a non-ADW employee, such as a consultant or software vendor.

## THIRD PARTY INFORMATION ASSETS

See “Information Assets”. Information that is not owned by ADW.

## TROJANS

A type of malware that is intended to damage or disable computers and computer systems.

## UNAUTHORIZED NETWORK INFORMATION GATHERING

Use of tools not sanctioned by the IT department to illicitly gather data or private information about networks, systems or applications.

## USB

The Universal Serial Bus is a standard, connectivity port on virtually all desktop computers and laptops, most commonly used to connect keyboards, mice and flash drives.

## VIRTUAL PRIVATE NETWORK

Abbreviated as VPN, this is a private network extended across a public network, such as the internet. VPNs allow employees to securely access corporate servers, and are frequently used to securely connect geographically separated offices of an organization, creating one cohesive network.

## VULNERABILITY SCANS

A form of penetration-testing that looks for weaknesses in security architecture.

## WORMS

A type of malware that is intended to damage or disable computers and computer systems.

# Acknowledgement of Receipt

*An original signed copy of this form is to be returned to the IT office.  
Retain a copy for your records.*

By signing below, I hereby acknowledge that I have received a copy of the Information Technology Security Policy and confirm that I have read the policy in its entirety and agree to comply with the policy. Failure to comply with the policy may result in termination of employment or termination of any contractual relationship.

\_\_\_\_\_

First name

MI

Last name

\_\_\_\_\_

Signature

\_\_\_\_\_

Name of Office/Program

Date

## **To Report a Security Concern**

To report a real or potential security concern, contact the Help Desk via email at [it@adw.org](mailto:it@adw.org) or phone at 301-853-4444, x444.

Submit a Help Desk request [it@adw.org](mailto:it@adw.org)

The Security Awareness presentation is available on the P: drive at: