Diocese of Pensacola-Tallahassee Guidelines on Anti-Virus Process

1.0 Overview

Discuss how to prevent computer infections using protective software as well as safe computing techniques. This is not to impose restrictions on computer users but to provide a standardized methodology to safeguard equipment used in the Diocese of Pensacola-Tallahassee.

2.0 Purpose

To outline measures to protect computers and data from viruses, malware, spyware and other destructive processes.

3.0 Scope

This policy applies to employees, volunteers, contractors, consultants, temporaries, and other workers at Diocese of Pensacola-Tallahassee, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Diocese of Pensacola-Tallahassee or personal equipment used to access diocesan systems, services, or equipment.

4.0 Policy

1. Always run Diocesan standard, supported anti-virus software. This is available for purchase through the Diocesan I.T. Department. Alternative products may be acceptable; check with the I.T. Department for approval. Install the current version; download and install anti-virus software updates as they become available.
2. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your email Trash folder.
3. Delete spam, chain, and other junk email without forwarding, in compliance with the Diocese of Pensacola-Tallahassee's *Acceptable Use Policy*.
4. Never download files from unknown or suspicious sources.
5. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so. This does not apply to server-based storage.
6. Always scan a flash drive for viruses before using it.
7. Back-up critical data and system configurations on a regular basis and store the data in a safe place.
8. If installation of a program conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the install. After the installation, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
9. If any unsolicited email message is received, regardless of the appearance, do NOT follow links, open attachments, or respond to the message. You can verify links contained within the message by placing your cursor on them to see actual linked web page address.
10. Do not install any pop-up updates to programs. Please verify with the I.T. Department before installing anything your computer.
11. Never share a password, personal information, bank or credit card information via email, regardless of the request. Confirm verbally with the requesting individual or entity their identity and reason for the request. Most such solicitations are fraudulent.
12. Always keep publisher-supported versions of operating systems installed on machines in use. The Diocesan I.T. Department recommends using the latest version of OS on any device. You can verify the version in use and coordinate upgrading with the I.T. Department at any time.

5.0 Enforcement

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

6.0 Definitions

Term	Definition
Attachment	A file which is sent along with an e-mail message.

Anti-virus software

A program that finds and removes viruses from a computer.

Operating System

An Operating System (or “OS”) is the software that allows a user to run other applications on a computing device. It also manages a computer's hardware resources, such as: keyboard, mouse, monitor, printers.

SPAM

E-mail spam, also known as junk e-mail, is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail.

7.0 Revision History

May 12, 2011: Section 4.6: update:
~~Thumb~~ flash drive
July 18, 2013: Section 4.0: Addition: If any unsolicited email message is received, regardless of the appearance, do NOT follow links, open attachments, or respond to the message. You can verify links contained within the message by placing your cursor on them to see actual linked web page address.
Do not install any pop-up updates to programs. Please verify with the I.T. Department before installing anything your computer.
March 19,2014: Section 4.5: added: “This does not apply to server-based storage.”
March 19, 2014: Section 4.6: deleted: from an unknown source
May 22, 2015: Section 3.0: Addition: **or personal equipment used to access diocesan systems, services, or equipment**
Sep 27, 2017L section 4.0.2: Change: ~~“your Trash”~~ **your email Trash folder**
Sep 27, 2017: Section 6.0: deleted: An e-mail attachment (or email attachment) is a computer
Sep 27, 2017: Section 4.0.11: Addition: **11. Never share a password, personal information, bank or credit card information via email, regardless of the request. Confirm verbally with the requesting individual or entity their identity and reason for the request. Most such solicitations are fraudulent.**
Sep 27, 2018: Reviewed
Jul 26, 2019: Section 4.0: Addition: **12. Always keep publisher-supported versions of operating systems installed on machines in use. The Diocesan I.T. Department recommends using the latest version of OS on any device. You can verify the version in use and coordinate upgrading with the I.T. Department at any time.**
Jul 26, 2019: Section 6.0: Addition: **Operating System definition.**