Diocese of Pensacola-Tallahassee Acceptable Use Policy

1.0 Overview
This Acceptable Use Policy is not to impose restrictions that are contrary to Diocese of Pensacola-Tallahassee's established culture of openness, trust, and integrity. The diocesan Information Technology Department is committed to protecting Diocese of Pensacola-Tallahassee's employees, volunteers and entities from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems provided by The Diocese, including but not limited to computer equipment, software, operating systems, storage media, PCD's, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Diocese of Pensacola-Tallahassee and/or its affiliated entities. These systems are to be used for business and ministerial purposes in serving the interests of the diocese in the course of normal operations.

Effective security is a team effort involving the participation and support of every Diocese of Pensacola-Tallahassee employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose
The purpose of this policy is to outline the acceptable use of computer equipment, services, and systems at Diocese of Pensacola-Tallahassee. These rules are in place to protect the employee and Diocese of Pensacola-Tallahassee. Inappropriate use and negligence expose the Diocese of Pensacola-Tallahassee to risks including virus attacks, compromise of network systems and services, and legal issues.

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 used for diocesan purposes.

4.0 Policy
4.1 General Use and Ownership
1. While Diocese of Pensacola-Tallahassee's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create or transmit using the diocesan systems remain the property of Diocese of Pensacola-Tallahassee. Because of the need to protect Diocese of Pensacola-Tallahassee's network, management cannot guarantee the confidentiality of information stored on any device belonging to Diocese of Pensacola-Tallahassee. While the diocese will not knowingly access or allow access to data created by diocesan users without prior permission, the I.T. Department will periodically perform scans on files for maintenance purposes and reserves the right to verify appropriateness of content.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult the I.T. Department.
3. For security and network maintenance purposes, authorized individuals within Diocese of Pensacola-Tallahassee may monitor equipment, systems and network traffic at any time.
4. Diocese of Pensacola-Tallahassee reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
5. Personal technology equipment used for diocesan purposes can be subject to the same supervision as diocesan assets.

4.2 Loss and Theft
1. Files containing confidential or sensitive data may not be stored in PCDs unless protected. Confidential or sensitive data shall never be stored on a personal PCD.
2. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the employee.
3. Lost or stolen equipment must immediately be reported.

4.3 Personal Use
All equipment, systems, and services are intended for use within the stated mission of the Diocese of Pensacola-Tallahassee. Personal use should be limited to minimal and incidental use. Data stored on diocesan equipment is considered property of the Diocese.

4.4 PCD Safety
Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If employees must use a PCD while driving, Diocese of Pensacola-Tallahassee requires the use of hands-free enabling devices, where state and local laws permit.

4.5 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: business strategies, client/parishioner-specific information, medical, payroll, insurance-related and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly and user level passwords should be changed every six months.
3. All PCs, laptops, PCD's, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the host will be unattended. Employees working in public areas and those working with confidential information should have screen saver timers set to less than five minutes.
4. Postings by employees from a Diocese of Pensacola-Tallahassee email address to newsgroups and/or social networking sites in the course of business duties must have approval of that material by their supervisor. Personal postings should never be done using a diocesan email account. If personal postings reference Diocese of Pensacola-Tallahassee, that posting shall contain a disclaimer stating that the opinions expressed are strictly their own and not those of Diocese of Pensacola-Tallahassee. For more specifics, refer to the *Diocesan Code of Conduct for Church Personnel and Volunteers*, section 3.6.3 "Personal Websites," section 3.6.4 "Blogs," and 3.6.5 "Inappropriate Language and Images."
5. All hosts used by the employee that are connected to the Diocese of Pensacola-Tallahassee Internet/Intranet/Extranet, whether owned by the employee or Diocese of Pensacola-Tallahassee, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy. Refer to the Diocese of Pensacola-Tallahassee Anti-Virus Guidelines policy for further details.
6. Employees and volunteers must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
7. Any unexpected pop-up messages on a computer screen should be ignored or shut down via an external process such as rebooting as it may be malware, a virus or Trojan horse code. Questions regarding suspicious program alerts or messages should be directed to the diocesan I.T. Department.
8. For system administrative purposes, the Diocesan I.T. Department may have access to passwords and secured systems. Extreme care to protect sensitive and/or personal information contained within those systems will be taken and confidentiality will be maintained by I.T. staff.

4.6 File Retention, Back-ups, Restoration

1. Files are separated into folders grouped by user, department, and general access. All documents, pictures, videos, etc. stored in any of these areas on our servers are backed up in a secured manner. Items stored on local drives are NOT backed up. Any data stored on a local or external drive are the sole responsibility of the owner. Any loss is not recoverable. Data retention policies of our diocese and the USCCB are to be followed.

2. Data retention policy is first dictated by guidelines provided by the USCCB. Individual departments may have additional requirements for length of retention. Your supervisor or department head should provide those instructions to you.
3. File-level backups of server data are made daily and maintained for two weeks.
4. Restores of data are requested through the I.T. Department and are usually completed within four business hours.

4.7 Password Guidelines

1. General Password Construction

Passwords are used for various purposes at Diocese of Pensacola-Tallahassee. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once,) guidelines for creating Strong Passwords include:

a) Contain both upper- and lower-case characters
b) Have digits and punctuation characters as well as letters
c) Are not based on personal information, names of family, etc.
d) Passwords should never be written down and only stored on-line if encrypted
e) Ideally are phrases

2. Password Protection Standards

a) Do not use the same password for Diocese of Pensacola-Tallahassee accounts as for other non-Diocese of Pensacola-Tallahassee access (e.g., personal ISP account, option trading, benefits, etc.).
b) Don't use the same password for various Diocese of Pensacola-Tallahassee access needs.
c) Do not share Diocese of Pensacola-Tallahassee passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive and confidential information of the Diocese and should only be shared with the diocesan I.T. Department staff.
d) If someone demands a password, refer them to this document or have them call the Information Technology Department.
e) Do not use the "Remember Password" feature of any web sites or web browsers.
f) Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY system (including portable devices) without encryption.
g) If an account or password is suspected to have been compromised, report the incident to I.T. Department and change all passwords.

4.8 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Any personnel with administrator access to a system do not automatically have the right to all information in that system. At all times, information should only be accessed if doing so is required by your job description. Ability to access information does not grant you the right to do so.

Under no circumstances is an employee of Diocese of Pensacola-Tallahassee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Diocese of Pensacola-Tallahassee -owned and/or managed resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. Performance of these activities can lead to disruption of normal work flow, data corruption or misuse, privacy violations and /or legal consequences.

4.8.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a) 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 Diocese of Pensacola-Tallahassee.
b) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Diocese of Pensacola-Tallahassee or the end user does not have an active license is strictly prohibited.
c) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
d) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
e) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
f) Using a Diocese of Pensacola-Tallahassee computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
g) Making fraudulent offers of products, items, or services originating from any Diocese of Pensacola-Tallahassee account.
h) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
i) Effecting 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.
j) Port scanning or security scanning is expressly prohibited unless prior notification to the diocesan I. T. Department is made.
k) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
l) Circumventing user authentication or security of any host, network or account.
m) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
n) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
o) Providing information about, or lists of, Diocese of Pensacola-Tallahassee employees to parties outside Diocese of Pensacola-Tallahassee or revealing personal information, such as the home address, telephone number, or Social Security number of another person or yourself.
p) Viewing and/or downloading of Non-Diocesan Business-Related Information including, but not limited to, entertainment, malicious, or pornographic content.
q) Printed materials containing personal or confidential information should be secured while not being actively used by authorized individuals. Documents containing sensitive information should be shredded if possible when no longer needed, or filed in secured locations as appropriate. Such printed materials should not be made available for viewing by anyone other than authorized personnel. Printed documents should be treated with the same discretion as digital copies of personal and/or confidential information. This treatment applies to draft as well as final copies."

4.8.2. Email and Communications Activities

a) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
b) Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

c) Unauthorized use, or forging, of email header information.
d) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
e) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
f) Use of unsolicited email originating from within Diocese of Pensacola-Tallahassee 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Diocese of Pensacola-Tallahassee or connected via Diocese of Pensacola-Tallahassee 's network.
g) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
h) Using diocesan email, email systems, network systems or Internet connectivity for personal, for-profit business activities.

4.8.3 Blogging, Tweeting or Similar

a) Blogging, tweeting or similar social media mass-postings by employees, whether using Diocese of Pensacola-Tallahassee's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Diocese of Pensacola-Tallahassee 's systems to engage in blogging, tweeting or similar activities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Diocese of Pensacola-Tallahassee 's policy, is not detrimental to Diocese of Pensacola-Tallahassee 's best interests, and does not interfere with an employee's regular work duties. Social media posting from Diocese of Pensacola-Tallahassee's systems is also subject to monitoring.
b) Diocese of Pensacola-Tallahassee's *Confidential Information Policy* also applies to social media posting. As such, Employees are prohibited from revealing any Diocesan confidential or proprietary information, trade secrets or any other material covered by Diocesan *Confidential Information Policy* when engaged in blogging.
c) Employees shall not engage in any social media posting that may harm or tarnish the image, reputation and/or goodwill of Diocese of Pensacola-Tallahassee and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when posting to social media or otherwise engaging in any conduct prohibited by Diocese of Pensacola-Tallahassee's Non-Discrimination and Anti-Harassment policy. Refer to Diocesan Human Resource department for descriptions of these policies.
d) Employees may also not attribute personal statements, opinions or beliefs to Diocese of Pensacola-Tallahassee when engaged in social media posting. If an employee is expressing his or her beliefs and/or opinions in social media venues, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Diocese of Pensacola-Tallahassee. Employees assume any and all risk associated with these social media postings.
e) Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Diocese of Pensacola-Tallahassee 's trademarks, logos and any other Diocese of Pensacola-Tallahassee intellectual property may also not be used in connection with any social media activity

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or criminal prosecution, as applicable.

If you suspect an employee, volunteer, contractor, or other person working within the diocese of violating this policy, refer to the *Diocesan Code of Conduct for Church Personnel and Volunteers*, section 8 "Reporting Ethical or Professional Misconduct" for the appropriate steps to take.

6.0 Definitions

Term	**Definition**
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Confidential or sensitive data	All data that is not approved for public release or that is legally considered to be personally identifiable information.
PCD	Personal Communication Device. This includes but is not limited to: pads, tablets, phones, and similar devices
Social Media	The means of interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Tweeting	Make a posting on the Twitter social networking site

7.0 Revision History

07/01/2010: section 4.3.2.h
~~Using diocesan email or email systems for personal, for-profit business activities~~
Using diocesan email, email systems, network systems or Internet connectivity for personal, for-profit business activities
May 5, 2011: section 1.0: update
The diocesan **Information Technology** Department is
section 4.1: delete
For security and network maintenance purposes, authorized individuals within Diocese of Pensacola-Tallahassee may monitor equipment, systems and network traffic at any time~~, per Diocesan I. T. Department's Audit Policy~~.
section 4.2: delete
The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines~~, details of which can be found in Human Resources policies~~.
Section 4.2: update
Because information contained on portable computers and removable storage devices (jump drives, thumb drives, etc.) is especially vulnerable, special care should be exercised. Protect laptops in accordance with ~~the "Laptop Security Tips."~~ **Mobile Computing and Portable Storage Device Policy.**
May 6, 2011: section 4.1: updated
1. The I.T. Department will periodically perform scans on files for maintenance purposes and maintains the right to verify appropriateness of content. While the diocese will not knowingly access or allow access to data created by diocesan users without prior permission, the I.T. Department will periodically perform scans on files for maintenance purposes and reserves the right to verify appropriateness of content.
April 26, 2012: section 1: addition

r) Viewing and/or downloading of Non-Diocesan Business Related Information including, but not limited to, entertainment or pornographic content.

May 1, 2012, Section 1.0: addition:
Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Diocese of Pensacola-Tallahassee **and/or its affiliated entities**.
May 1, 2012: Section 5.0: addition:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment **and/or criminal prosecution as applicable**.
August 21,2012: Section 4.3.1 (o): addition: Providing information about, or lists of, Diocese of Pensacola-Tallahassee employees to parties outside Diocese of Pensacola-Tallahassee **or revealing personal information, such as the home address, telephone number, or Social Security number of another person or yourself.**
July 18, 2013: Section 4.1 (1): Delete: any ~~network~~ device
July 18, 2013: Section 4.1 (3): Delete: any information ~~that~~ users consider. ~~For guidelines on information classification, see the Diocesan I. T. Department's Information Sensitivity Policy.~~
July 18, 2013: Section 4.1 (3) change: documents, ~~go~~ refer to Diocesan
July 18, 2013: Section 4.2 (2): Addition: Refer to *Diocesan Password Policy.*
July 18, 2013: Section 4.2 (3) Delete: by logging-off ~~(control-alt-delete for Win2K users)~~ when the host
July 18, 2013: Section 4.2 (5): Change: ~~jump~~ flash Mobile ~~Computing and Portable Storage Device Policy~~ Portable Device Policy
July 18, 2013: Section 4.3: Addition: Diocese of Pensacola-Tallahassee -owned and/or managed resources
July 18, 2013: Section 4.3: Addition: Refer to Diocesan Human Resource department for descriptions of these policies.
July 18, 2013: Section 4.4: Change: ~~Blogging~~ Blogging, Tweeting, or similar
July 18, 2013: Section 4.4 (1) 1.Addition: Blogging, tweeting or similar social media mass-postings by employees
July 18, 2013: Section 4.4 (3) Change: ~~blogging,~~ social media posting
March 19, 2014: Section 4.2(1): delete: The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines.
Examples of confidential information include but are not limited to: business strategies, client/parishioner-specific information, medical, payroll, insurance-related and research data.
May 22, 2015: Section 1.0: addition: Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, **PCD's,** network accounts providing electronic mail, WWW browsing, and FTP, are the

property of Diocese of Pensacola-Tallahassee and/or its affiliated entities. These systems are to be used for business **and ministerial** purposes in serving the interests of the diocese in the course of normal operations.
May 22, 2015: Section 2.0: Addition: outline the acceptable use of computer equipment**, services, and systems** at
May 22, 2015: Section 2.0: Addition: **and negligence**
May 22, 2015: Section 3.0: addition: **or used for diocesan purposes.**
May 22, 2015: Section 4.1/1: Delete & renumber: The diocesan I. T. Department recommends that any information users consider sensitive or vulnerable be encrypted. For guidelines on encrypting email and documents, refer to Diocesan I.T. Department's Acceptable Encryption Policy.
May 22, 2015: Section 4.2/2: Delete: Refer to diocesan *Password Policy.*
May 22, 2015: Section 4.2/4: Delete & renumber: Use encryption of information in compliance with Diocesan I. T. Department's Acceptable Encryption Use policy.
May 22, 2015: Section 4.2/5: Delete & renumber: Because information contained on portable computers and removable storage devices (flash drives, thumb drives, etc.) is especially vulnerable, special care should be exercised. Protect laptops in accordance with the Portable Device Policy.
May 22, 2015: Section 4.3: Change: renumber to 4.4,
May 22, 2015: Section 4.3: Addition: of Password Guidelines from former stand-alone "Password Policy" document
May 22, 2015: Section 4.3/2-c:Change: a) Do not share Diocese of Pensacola-Tallahassee passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated **as sensitive and information of the Diocese and should only be shared with the diocesan I.T. Department staff.** ~~The I.T. Department can grant access to shared mailboxes, folders and the like as necessary~~.
Sep 26, 2017: Section 4.1 Addition: **5. Personal technology equipment used for diocesan purposes can be subject to the same supervision as diocesan assets.**
Sep 26, 2017: Section 4.5.3: Change: ~~set at 10 minutes or less~~ set at 15 minutes or less
Sep 26, 2017: Section 4.5.3: Change: ~~less than one minute.~~ less than five minutes.
Sep 26, 2017: Section 4.5.4: Addition**: . For more specifics, refer to the Diocesan Code of Conduct for Church Personnel and Volunteers, section 3.6.3 "Personal Websites," section 3.6.4 "Blogs," and 3.6.5 "Inappropriate Language and Images."**
Sep 26, 2017: Section 4.5.7: Addition: **Questions regarding suspicious program alerts or messages should be directed to the diocesan I.T. Department.**
Sep 26, 2017: Section 4.6.1: Addition: **(e) Ideally are phrases**
Sep 26 ,2017: Section 4.6.2: Delete: ~~At the Diocese of Pensacola-Tallahassee Pastoral Center, one password will grant access to the network and your email; for this reason, you should never share this password with anyone else.~~
Sep 26, 2017: Section 5.0: Addition: **If you suspect an employee, volunteer, contractor, or other person working within the diocese of violating this policy, refer to the Diocesan Code of Conduct for Church Personnel and Volunteers, section 8 "Reporting Ethical or Professional Misconduct" for the appropriate steps to take**
Sep. 27, 2018: Sec. 1.0: Change**:** ~~"trust,and.~~" **trust, and**
Sec 1.0: Addition: ~~Internet/Intranet/Extranet-related systems,~~ **Internet/Intranet/Extranet-related systems provided by The Diocese,**
Sec 4.1: Change: ~~using the corporate~~ **using the diocesan**
Sec. 4.7.1: Addition: "q. Printed materials containing personal or confidential information should be secured while not being actively used by authorized individuals. Documents containing sensitive information should be shredded if possible when no longer needed, or filed in secured locations as appropriate. Such printed materials should not be made available for viewing by anyone other than authorized personnel. Printed documents should be treated with the same discretion as digital copies of personal and/or confidential information. This treatment applies to draft as well as final copies."
Mar. 20, 2019: section 4.6: Addition: **4.6 File Retention, Back-ups, Restoration**
Mar. 20, 2019: section 4.7: Change: renumbered from 4.6
Mar. 20, 2019: section 4.8: change: renumbered from 4.7
Jul. 26, 2019: section 2.0: Change: **expose the**
Jul. 26, 2019: section 4.5.5: Addition: **Refer to the Diocese of Pensacola-Tallahassee Anti-Virus Guidelines policy for further details.**
Jul. 26, 2019: section 4.7.1a: Change: upper and lowercase to **upper- and lower-case**
Jul. 26, 2019: section 4.7.2e: Addition: **or web browsers**
Jul. 26, 2019: section 4.8.1p: Addition: **malicious,**
Jul. 26, 2019: section 4.5.8: Addition: **For system administrative purposes, the Diocesan I.T. Department may have access to passwords and secured systems. Extreme care to protect sensitive and/or personal information contained within those systems will be taken and confidentiality will be maintained by I.T. staff.**