The Network Acceptable Use Policy
for all Parishes, Schools, and Entities of the Diocese of St. Augustine
Updated: April 30, 2018

1.0 Glossary of Terms

1.1 Authorized users

1. "Employee:" Any layperson who is employed by or engaged in ministry in any diocesan entity, whether part-time or full-time, who is given payment for services rendered, and for whom the diocesan entity is obligated to withhold payroll taxes (FICA, Medicare, and withholding).

2. "Volunteer:" Any unpaid person engaged or involved in a diocesan activity, specifically as it relates to database creation and/or management, IT services, or internet-related services.

3. "Church Personnel:" For purposes of this policy only, Church Personnel includes all individuals who minister, work, or volunteer in any school, parish, or ministry of the diocese whose compliance with this policy is required. The term has no legal meaning or significance outside the scope of this policy and is not indicative of any employment or agency relationship.

4. "Consultant:" Independent contractors, consultants, vendors or other persons who are not subject to the supervision of the Bishop of the Diocese of St. Augustine and for whom no such duty to withhold payroll taxes exist, but provide expertise on database creation and/or management, IT services, or internet-related services.

1.3 Internet/Intranet/Extranet-related systems

These systems include, but are not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, World Wide Web browsing and FTP.

1. All Internet/Intranet/Extranet-related systems are the property of the diocesan entity it serves. These systems are used for business purposes in serving the interests of the diocesan entity, its staff, and its constituents in the course of its normal operations.

1.4 Diocesan entity

Any parish, school, entity or ministry of the Diocese of St. Augustine, including those entities which are separately incorporated under 501(c) (3).

1.5 Personally Identifiable Information (PII)

Any information about an individual that can be used to distinguish or trace a person's identity. PII is defined as any one or more of types of information including, but not limited to:

1. Social Security number
2. Username and password
3. Passport number
4. Credit card number
5. Clearances
6. Banking information
7. Biometrics
8. Data and place of birth
9. Mother's maiden name
10. Criminal, medical and financial records
11. Educational transcripts
12. Photos and video including any of the above

All electronic files that contain PII will reside with the diocesan entity's physically secure location. All physical files that contain PII will reside within a locked file cabinet or room when not being actively viewed or modified.

PII is not to be downloaded to workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or systems outside the protection of the diocesan entity. PII will also not be sent through any form of unsecured electronic communication as significant security risk emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII, the physical or electronic file should be shredded or securely deleted. Authorized diocesan personnel will do all disposal of PII.

All PII will be collected only when there is a legal authority, and it is necessary to conduct diocesan business.

Access to PII is only conducted when the information is needed to conduct official diocesan business and should only be utilized for official purposes. Authorized users will not create duplicate copies of documents that contain PII and will destroy the documents when no longer needed. When PII is extracted from a document, authorized users may only target the PII that is required for the task. PII that is extracted shall not be retained beyond the records retention rules for the data and the system it was accessed from. PII shall not be stored or transmitted via personally owned devices. PII may not be taken home by any authorized user.

1.6 Personally Owned Information Systems

Personally owned devices include cell phones, tablets or any other device that is owned and maintained by the user, not the diocesan entity.

Personally owned devices are not allowed to access the diocesan entities network. Therefore, a device that is not owned by the Diocese of St. Augustine shall not process, store, access or transmit data or confidential information.

Under no circumstances are users allowed to connect their personal device to a diocesan entity network or any diocesan-owned devices, applications or systems.

1.7 Spam
Unauthorized and/or unsolicited electronic mass mailings.

1.8 IT
Information Technology

1.9 Internet
Includes both external and internal access of communications and data storage equipment, either owned or reserved for use by the diocese, by digital information devices including personal computers (PCs), personal digital assistants (PDAs) and similar devices. The term "Internet," as it applies to external resources, is meant to be all-inclusive and comprises other similar or analogous terms such as the "World Wide Web," "email," and "the Net."

1.10 Network
A communications system connects two or more computers and their peripheral devices to exchange information and share resources. For this policy, this also includes stand-alone computers.

2.0 Overview
The Diocese of St. Augustine recognizes that the Network/Internet and other emerging technologies allow authorized users access to immense information globally. The Diocese of St. Augustine's goal in providing this privilege to authorized users is to promote professional excellence, innovation, and communication. The use of the Network/Internet or other emerging technologies will be guided by the Diocesan Network Acceptable Use Policy (DNAUP). All Diocese of St. Augustine authorized users are required to sign a written DNAUP and to abide by the terms and conditions of the policy and its accompanying regulations.

3.0 Scope
This policy applies to authorized users of any school, parish or ministry of the Diocese of St. Augustine, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or used by the diocesan entity.

4.0 Purpose
The purpose of this DNAUP is not to impose restrictions that are contrary to an established culture of openness, transparency, trust, and integrity. Rather, the Diocese of St. Augustine is committed to protecting its authorized users from illegal or damaging actions by individuals, either knowingly or unknowingly.

These rules are in place to protect authorized users and diocesan entities. Inappropriate use exposes diocesan entities to risks including virus attacks, compromise of network systems and services and legal issues. Anyone with knowledge of inappropriate material/content should report this information verbally and in writing to the IT authority or the principal, pastor, or layperson in charge of the school, parish or ministry of the diocese.

5.0 Policy

5.1 General Use and Ownership

1. Authorized users should be aware that the data they create on systems remains the property of the diocesan entity. Because of the need to protect the network, management cannot guarantee the confidentiality of information stored on any network device belonging to a diocesan entity.

2. Authorized users are responsible for exercising good judgment regarding the use of network/computer systems. Authorized users should be guided by diocesan policies on personal use, and if there is any uncertainty, authorized users should consult their supervisor or manager.

3. The Diocese of St. Augustine recommends that any information that users consider sensitive or vulnerable be encrypted, especially when stored on external media.

4. Authorized personnel, acting on behalf of the Diocese of St. Augustine, may monitor equipment, systems, and network traffic at any time. The Diocese of St. Augustine maintains the right to monitor all network/computer activity derived from or utilized through its resources, whether it is online, downloaded or through printed material.

5. The Diocese of St. Augustine, through its entities, reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

6. All data and files on network/computer systems are the property of the Diocese of St. Augustine.

5.2 Security and Proprietary Information

1. Anyone responsible for entering information into a database or having access to database information used by any diocesan entity, whether clergy, religious, employee or volunteer, must be FBI fingerprinted and background checked and cleared.

2. The appropriate IT authority of each diocesan entity does everything possible to ensure the diocesan entity network is properly maintained and adequate security measures are operational. To assist the appropriate IT authority of each diocesan entity in sustaining this goal, authorized users, through their supervisor, should notify their IT authority when software and hardware modifications are necessary on any diocesan computer workstation. At no time should a computer be connected to a diocesan entity network without the approval of the IT authority of the diocesan entity.

   The user interface for information contained on Internet/Intranet/ Extranet-related systems should be classified as either confidential or not confidential, as defined by school confidentiality guidelines. Staff and students should take all necessary steps to prevent unauthorized access to this information.

3. **Password Policy**

Passwords will be created by each authorized user for their own use, with the exception of students, volunteers, and temporary/contractual personnel.

Authorized user passwords shall not be shared. It is the responsibility of each authorized user to keep his/her password confidential. Anyone whose password becomes known to another person should notify the IT authority immediately, and a new password will be created. Anyone who becomes aware of anyone else's password should contact the IT authority immediately, and a new password will be created.

Temporary passwords used by students, volunteers or temporary/contractual personnel may be known by the supervisor and other appropriate authorities. However, temporary passwords should not be shared. System server level passwords should be changed quarterly by the IT authority; user level passwords should be changed at least every 90-days.

4. **Authentication Strategy**

This Password Policy applies to all information systems and applications that contain or access the diocesan entity's information or services. This includes, but is not limited to:

- Mainframes, servers and other devices that provide centralized computing capabilities
- SAN, NAS and other devices that provide centralized storage capabilities.
- Diocesan issued desktops, laptops, or any other device that provides distributed computing capabilities.
- Routers, switches and other devices that provide network capabilities.
- Firewalls and other devices that provide dedicated security capabilities.
- Windows Domain Accounts, diocesan email accounts, diocesan entity application accounts as well as any other information system or service.

The diocese dictates that each password and User-ID be unique and not be shared with any other individual. Users are forbidden to share their unique password or write it down. All passwords must be memorized.

Each user who is authorized to access, store, process, administer and maintain the system, applications and data must be uniquely identified.

If personnel are on the diocesan entity's network, a username and password are required. All passwords should:

- Not contain significant portions of the user's account name or full name.
- Be at least eight (8) characters in length.
- Contain characters from three of the four categories:
  - English uppercase characters (A to Z)
  - English lowercase characters (a to z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (!, $, #, %, etc.)

- Not be the same as the username.
- Changed within a maximum of 90 calendar days.
- Not be identical to the previous ten (10) passwords.
- Must consist of 1 uppercase letter, 1 number, 1 special character.
- Not be displayed when entered.

a. All PCs, laptops, 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 (control-alt-delete for Windows 7 Professional and above users) when the host will be unattended.

b. Due to the vulnerability of external media, such as flash drives, special care should be exercised to protect systems from damaging viruses in accordance with this policy. Authorized users are required to obtain supervisor approval before using, transmitting or taking files off-site. Information considered sensitive and of a confidential nature, such as personnel files and payroll data, are not permitted to leave the work site for any reason.

c. Postings by authorized users from any diocesan email address to online bulletin boards, forums, chat rooms, web logs ("blogs")" and any other similar non-work-related discussion groups are prohibited, unless they are specifically work-related.

d. All hosts used by the authorized user that is connected to any diocesan Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database.

e. Authorized users must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

f. Consult with your IT authority before sending “blast” emails. Sending an email to more than 100 recipients at a time is considered a “blast” email. The diocese discourages this practice unless an outside vendor is used to manage the dissemination of such emails.

g. Whenever sending “blast” emails or emails to many recipients, use the blind copy (bc) for the recipients to ensure respect for the privacy of each address.

5. **Incident Response for Desktop and Mobile Data Terminal (MDT) Computers**
If an incident occurs involving any device (workstations, smartphones, laptops, tablets, etc.) that is on a diocesan entity network, the appropriate supervisor shall be contacted immediately. If it is deemed by the supervisor to be a security breach of confidential information, a Security Incident Response Form will be completed.

All users are responsible for reporting known or suspected information or information technology security incidents. All incidents must be reported immediately to the

appropriate supervisor. The supervisor will inform the IT authority and document the incident.

The diocesan entity will employ on all desktop and laptop devices and will ensure that the antivirus software is up-to-date.

Incident response will be managed based on the level of severity of the incident. The level is a measure of its impact or threat on the operation or integrity of the Diocese of St. Augustine and its' information. High Level (potential to impact the network or data) Medium Level (potential to impact one system or non-critical system) Low Level (has little or no risk of infecting the network or system).

The diocesan entity will identify the security breach by conducting the following:

a. Confirm the discovery of a compromised resource(s).
b. Evaluate the security incident.
c. Identify the system(s) of information affected.
d. Review all preliminary details.
e. Characterize the impact on the diocesan entity as: minimal, serious, or critical.
f. Determine where and how the breach occurred.
    a. Identify the source of the compromise and the time frame involved. Review the network to identify all compromised or affected systems.
g. Examine appropriate system and audit logs for further irregularities.
    a. Document all internet protocol (IP) addresses, operating systems, domain system names and other pertinent system information.
h. Initiate measures to contain and control the incident to prevent further unauthorized access.
i. Document actions through the process from initial detection to final resolution.

5.3 Unacceptable Use

1. A database of subscribers for parish or other diocesan entities can be a useful tool for parish or entity distribution of important messages, calendar of events, or other data. The marketplace is full of companies that offer such database opportunities. This type of database can also compromise a person's identity and/or place an individual in danger if the database is misused, compromised or shared indiscreetly. No parish or diocesan entity should create or subscribe to a vehicle by which subscribers, other than authorized personnel such as employees, priests, deacons, religious or those designated at the discretion of the pastor or head of the diocesan entity, are given email addresses to communicate with other subscribers. This does not apply to instructional technology or methodology which includes approved subscriber access for a specific instructional purpose and is monitored for this purpose. This instructional technology should not offer chat or chat rooms separate from the monitored purpose. Also, the application should NOT:
    a. Allow blogs
    b. Require or request photos of subscribers
    c. Ask for age or gender of subscribers
    d. Display subscriber email addresses

e. Allow subscribers access to other subscriber information

As we utilize the Internet, email and other technology for communication, we must be aware of the serious and grave danger to our children and young people when information is misguided or given innocently to the wrong people.

2. The following activities are, in general, prohibited. Authorized users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services).
    a. Under no circumstances is an authorized user allowed to engage in any activity that is illegal under local, state, federal or international law while utilizing the diocesan entity-owned resources.

    b. Authorized users are prohibited from attempting to circumvent or subvert any system's security measures. Authorized users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

    c. When an authorized user becomes "unauthorized" by employment, dismissal, graduation, retirement, etc., or if the authorized user is assigned a new position and/or responsibilities within the diocese, his/her access authorization will automatically be reviewed with the appropriate individual to determine whether continued access is warranted. This person may not use facilities, accounts, access codes, privileges or information for which he/she has not been authorized.

3. **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 the diocesan entity.

    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 the diocesan entity or the end user does not have an active license is strictly prohibited. Public disclosure of information about programs (e.g., source code) without the owner's authorization is 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 before export of any material that is in question.

    d. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

e. Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.

f. The installation or use of Instant Messaging is prohibited without prior approval from the appropriate department directory.

g. The installation or use of Instant Messaging is prohibited.

h. Using a diocesan computing asset to access inappropriate or offensive material or to engage in the procuring or transmitting of material that violates diocesan anti-harassment or hostile environment policies.

i. Making fraudulent offers of products, items or services originating from any diocesan entity account.

j. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

k. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the authorized user is not an intended recipient or logging into a server or account that the authorized user 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, creating or propagating viruses, hacking, network sniffing, spamming, pinged floods, packet spoofing, password grabbing, disk scavenging, denial of service and forged routing information for malicious purposes.

l. Port scanning or security scanning is expressly prohibited unless prior notification is made to the Diocese of St. Augustine.

m. Executing any form of network monitoring which will intercept data not intended for the authorized user's host, unless this activity is a part of the authorized user's normal job duty.

n. Circumventing user authentication or the security of any host, network or account.

o. 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.

p. Posting photos, digital video, and other personal information of children and diocesan personnel, without authorization, to Internet sites is prohibited. This includes, but is not limited to, activities that are conducted on personal computer equipment off-site and after working hours.

q. Peer-to-Peer file sharing. This includes, but is not limited to, Lime wire, Morpheus, and Napster.

4. **Employee Responsibilities**

Privacy: No authorized user should view, copy, alter or destroy another's personal electronic files without permission.

Harassment, Libel, and Slander: Under no circumstances, may any authorized user use Diocese of St. Augustine computers or network resources to libel, slander or harass any other person.

Abuse of Computer Resources: Abuse of Diocese of St. Augustine computer resources is prohibited. This abuse includes, but is not limited to, the following:

1. Unauthorized use of software: Software downloaded from the Internet or loaded from disks and flash drives are prohibited unless approved by the IT authority.

2. Game Playing: Installing or playing recreational games, which is not part of authorized and assigned job-related activity, are considered unacceptable practices and are prohibited.

3. Chain Letters: The propagation of chain letters (email), "Ponzi" or other "pyramid" schemes of any type are considered an unacceptable practice and are prohibited.

4. Unauthorized Servers: The establishment of a background process that services incoming requests from anonymous diocesan employees for purposes of music/radio/video continuous Internet connectivity, chatting or browsing the Internet is prohibited.

5. Unauthorized Monitoring: An employee may not use computing resources for unauthorized monitoring of electronic communications of other employees.

6. Private Commercial Purposes: Personal use of network and computer resources of the Diocese of St. Augustine is prohibited.

5.4 Email and Communications Activities

Diocesan entities maintain electronic mail systems. These systems are provided by the diocesan entity to assist in conducting business within the diocese.

1. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages is not allowed.

2. Unauthorized use, or forging, of email header information, is not allowed.

3. Solicitation of email for any other email address with the intent to harass or to collect replies from an email other than that of the poster's account is not allowed.

4. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam) is not allowed.

5. The electronic mail system hardware is the property of the diocesan entity. Additionally, all messages composed, sent or received on the electronic mail system are and remain the property of the diocesan entity. The diocese, through the appropriate authority, reserves the right to review, audit, intercept, and access all messages created, received or sent over the electronic mail system for any purpose.

6. The email system was created to facilitate operations of the diocesan entity. It should be used primarily for business purposes, and only incidentally for personal use. Likewise, personal email through such networks as AOL, Yahoo, Gmail, and others should be accessed on a limited basis, unless those networks are being used for diocesan business.

7. The electronic mail system may not be used to solicit or proselytize for commercial ventures, political causes, outside organizations or other non-job related solicitations.

8. The electronic mail system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone’s age, sexual orientation, religious or political beliefs, national origin, disability, veteran or marital status.

9. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

10. Notwithstanding the diocese’s right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other authorized users and accessed only by the intended recipient. Authorized users are not authorized to retrieve or read any email messages that are not sent to them.

11. Authorized users shall not use a code, access a file, or retrieve any stored information unless authorized to do so. Authorized users should not attempt to gain access to another authorized user’s messages without the latter’s permission.

12. All authorized users should perform routine maintenance of their mailboxes and delete messages they are no longer using.

13. The appropriate authority should be notified if a user becomes aware of emails which violate this policy.

14. Extreme care should be exercised when sending emails with sensitive information because a majority of email systems are not encrypted and secure.

6.0 Enforcement

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

The Diocese of St. Augustine does not sanction any use of the Network/Internet and other available technology that is not authorized by or conducted strictly in compliance with this policy and its regulations. Authorized users who disregard the DNAUP may have their Network/Internet privileges suspended or revoked and may be subject to appropriate corrective action, up to and including termination.

The Diocese of St. Augustine reserves the right to suspend or revoke such privileges if any supervisor believes the authorized user's conduct to be inappropriate or noncompliant with the DNAUP.

Authorized users granted access to the Network/Internet, and other technologies through the Diocese of St. Augustine assume personal responsibility and liability, for their actions. Also, any employee, volunteer, or contractor found to have violated this policy may be subject to corrective action, up to and including termination.

Authorized users who have read and signed the DNAUP form and who agree to act in a considerate and responsible manner will be authorized Network/Internet access.

7.0 System Back-up(s)

Although the diocesan entity should provide system back-ups as a standard operating procedure, it is the responsibility of each authorized user to back up his/her specific computer workstation data. Depending upon the amount of the individual workstation usage, workstation backups should occur daily.

8.0 Virus Protection

All networked computers must have current virus protection software, operating system updates, such as Windows updates, installed and operational at all times. Windows updates should occur at least monthly.

Patch Management

All workstations, mobile devices and servers owned by the Diocese of St. Augustine must have up-to-date operating system security patches installed in order to protect the device and network from known vulnerabilities.

Workstations, desktops and laptops have automatic updates enabled for the operating system patches. Current diocesan entity servers have the minimum baseline requirements that define the default operating system level, service pack, hotfix, and patch level required to ensure the security of diocesan data and networks.

IT will manage the patching needs for the servers on the network. In addition, they will manage the patching needs for all workstations on the network. IT will routinely assess the compliance of the patching policy and will provide guidance to all personnel of any security and patch management issues. IT also approves monthly and emergency patch deployments if necessary.
IT will monitor and report the outcome of each patching cycle. If a patch is causing vulnerability on the network or appliance, IT will roll the patch back in order to lessen the chance of vulnerabilities on the network.

The diocesan IT authority shall review all security relevant patches, service packs, and hot fixes from the vendors. Once reviewed, the patches will be fixed promptly.

9.0 Website Requirements

Diocesan entity websites are not permitted to link to other websites that conflict with church teaching and the Magisterium of the Roman Catholic Church. Permissible links fall into these main areas:

1. Official Church sites, such as the Vatican, United States Conference of Catholic Bishops, state conferences, archdioceses, and dioceses;

2. Parts of the diocese such as parishes, schools and ministries operated by the diocese or approved resources associated with those ministries; and

3. Under the oversight of a bishop or religious congregation, or listed in the Official Catholic Directory. Church leaders should use prudence in evaluating links to other commercial opportunities on its site. It is the diocesan entity's responsibility to evaluate its hosts' advertisers and sponsors on a regular basis.

4. Use of photos on websites should be group photos. Where children are involved, first names only should be used. Parents/guardians must sign permission slips each year for the use of children's photos; therefore, all photos, particularly those which include children, should regularly be refreshed.

5. Approved websites by diocesan entities should post the following disclaimer to the homepage of each site:

   "Although links to and from this website are frequently monitored for content, anyone who finds inappropriate content should immediately notify the [diocesan entity], so the link may be reviewed and/or removed."

6. All diocesan parishes, schools, and entities should have a link to the Diocese of St. Augustine website, www.dosafl.com, on its own website.

7. Diocesan entities, except parishes and schools, must obtain approval from their supervisor and/or the Director of Communications before establishing a website.

10.0 To provide interactive service, diocesan entities may collect personally-identifiable information from the users of the website. If such information is collected, the user will be informed about this practice. Additionally, if a website is directed to children or if a general audience website collects personal information from children, the diocesan entity must comply with the Diocese of St. Augustine online privacy policy. The privacy policy is attached and also posted on the Diocese of St. Augustine website under policies and procedures at www.dosafl.com.

ADDENDUM

"Best Practices"

Computer Security and Virus Protection:

- Install anti-virus software and keep it up-to-date. Refer all questions to the IT authority of the diocesan entity.
- Be cautious when opening email attachments

Content Filters

1. Content filtering is the blocking of content based on a rating system that is static, dynamic or a combination of both. Several content filtering products use a remote database of previously classified sites or IP addresses in conjunction with a local cache of frequently or recently requested sites. Some use a dynamic rating system that evaluates the content on the fly. Newer dynamic rating technologies offer more protection and use context-based rules instead of relying only on single keyword blocking.

2. All content filtering products will have about a dozen different content categories, such as Violence, Pornography, Hate/Racism, Nudity, and so on.

3. Some content filter manufacturers you may be familiar with include SonicWall, WatchGuard, Websense, SurfControl, and Symantec. These products offer gateway control; there are numerous client-based products available that load on the desktop, but capabilities are limited and management is difficult for a network with even a handful of PCs.

Electronic Media Sanitization and Disposal

1. Electronic media that has reached the end of its lifecycle must be sanitized and disposed of to ensure that confidential information is not viewed or accessed by unauthorized individuals. Electronic media is defined as any electronic storage device that is used to record information, including, but not limited to: hard disks, magnetic tapes, compact disks, videotapes, audiotapes, and removable storage devices such as USB drives.

2. All electronic media must be properly sanitized before being transferred from the custody of the diocesan entity. The proper method of sanitization depends on the type of media and the intended disposition of the media.

3. Hard Drives: The diocesan entity will overwrite the hard drive utilizing a three-pass wipe and/or physically destroyed. This will ensure that the data on the drive is overwritten with patterns of binary ones and zeros. The sanitization of the hard drive is not complete until the third wipe passes and a verification pass is complete.

4. Destruction of the hard drive will be conducted onsite by the document destruction vendor of the diocesan entity. This will be carried out or witnessed by authorized personnel of the diocesan.

5. USB drives, floppy disks, rewritable CD-ROMS, zip disks, videotapes, hard drives and audiotapes will be erased if able and then destroyed by drilling or smashing, witnessed or carried out by authorized personnel of the diocese.

Media Protection

1. Media in all forms shall be protected at all times.

2. Digital and physical media is restricted to authorized individuals. Only those users of the diocesan entity who have appropriate training will be allowed to access diocesan information or data in any form.

3. Handling physical media – The Diocese of St. Augustine will ensure that only authorized individuals will be granted access to media containing confidential information.

4. The media will be stored within a physically secure building and kept behind locked doors and locked cabinets. When no longer needed, the electronic media will be disposed of by the IT authority of the diocesan entity. Hard copies will be disposed of by authorized agency personnel only by depositing the hard copies into the locked receptacle for document shredding by the vendor of the diocese.

5. When it comes time for onsite shredding by the contracted vendor, authorized personnel of the diocesan entity will witness that shredding by the document destruction vendor.

6. Any media that is transported outside the physically secure location will be kept in a sealed envelope to ensure security is kept. When the media is released to another user, the user will document the transaction in a secondary dissemination log for validation purposes.

7. At no time will the physical media be released to an unauthorized person or left without proper documentation.

Minimum telecommunications closet size

Include space for an uninterruptible power supply in each closet. There should be a minimum of two electrical circuits in each closet. Design for good even lighting throughout the entire closet space both high and low. And finally, provide for enough cooling capacity for the electronics in the room.

Make sure there is some access control, and they are not open to the public.

Phishing and Spam

Follow these guidelines to avoid scams that can potentially infect your computer and the network:

- Be suspicious of any email or communication (including text messages, social media posts, ads) with urgent requests for personal financial information.

- Phishers typically include upsetting or exciting (but false) statements to get people to hand over their usernames, passwords, credit card numbers, Social Security numbers, date of birth and other personal information. Do not reply to any email without verifying the identity of the sender. Check the reply-to-email address and contact the sender directly to verify. Most phishing emails will come from a display name you recognize.

- Avoid clicking on links. Instead, go to the website by typing the web address directly into your browser or by searching for it in a search engine. Calling the company to verify its legitimacy is also an option, too.

- Pay attention to the website you are being directed to and hover over URLs. An email that appears to be from PayPal could direct you to a website that is instead http://www.2paypal.com or "hxxp://www.gotyouscammed.com/paypal/login.htm.

Physical Protection

1. Only authorized personnel have access to the Catholic Center and the Father Felix Varela Center. The buildings are equipped with key access for diocesan personnel. Visitors must sign in at the front desk of the Catholic Center. The Diocese of St. Augustine has a policy that non-agency guests are to be escorted by diocesan personnel to the office or department of the person they are scheduled to meet with. When escorted into the buildings, visitors must be accompanied by an authorized staff member.
2. All computer screens will be turned away from public view.
3. All physical media containing confidential information or data will be locked in filing cabinet in a locked office. Only authorized personnel will have a key to the cabinet.
4. All computer components will be locked in the secure server room. Only IT will have access to the server room. All vendors and contractors will undergo fingerprint-based records checks and will complete appropriate security awareness training.

Secure Network Closets

When designing and building telecommunications closets make sure that they are:

- At least One Closet Per Floor
- A safe working environment
- Provide enough space for today's technology as well as the potential for scalability.

Spyware

Spyware installs itself onto a user's computer by stealth, subterfuge and/or social engineering and sends information from that computer to a third party without the user's permission or knowledge. Spyware includes keyloggers, backdoor Trojans, password stealers, and botnet worms, which cause corporate data theft, financial loss, and network damage. To protect your computers against it, the computers utilizing your network need to have a spyware detection program. Good anti-virus programs can detect and remove spyware programs, which are treated as a type of Trojan.

System Backup

- Develop backup and restore strategies and test them. With a good plan, you can quickly recover your data if it is lost.

- Back up all data on the system and boot volumes and the System State. This precaution prepares you for the unlikely event of a disk failure.

- Create a backup log. Keep a book of logs to make it easier to locate specific files.

- Retain copies. Keep at least three copies of the media. Keep at least one copy off-site in a properly-controlled environment.

- Perform trial restorations to verify that your files were properly backed up. A trial restoration can uncover hardware problems that do not show up when you verify software.

- Secure devices and media. It is possible for someone to access the data from a stolen medium by restoring the data to another server for which they are an administrator.