1. Overview

The Diocese of Greensburg, which includes the Pastoral Center, its affiliated parishes and schools, and Catholic Charities, is committed to protecting its employees, volunteers, partners and the organization at large from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, private cloud computing accounts, network accounts providing electronic mail, Web browsing, and FTP, are the property of the Diocese. These systems are to be used for business purposes in serving the interests of the organization, our parishioners, parents and students and partners in the course of normal operations.

Effective security is a team effort involving the participation and support of every diocesan employee, volunteer 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. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and systems at the diocese. These rules are in place to protect the employee and the organization. Inappropriate use exposes all of us to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct diocesan, parish, school and Catholic Charities' business or interact with internal networks and business systems, whether owned or leased by the organization, the employee, or a third party. All employees, contractors, consultants, volunteers, temporary, and other workers at the diocese and its affiliated parishes, schools and Catholic Charities are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the Diocese of Greensburg policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Diocese of Greensburg, including all personnel affiliated with third parties. This policy applies to

all equipment that is owned or leased by the Diocese of Greensburg or that is connected to the Diocese of Greensburg WAN known as HALO.

Please note that because the Diocese of Greensburg users may access a number of computer networks, acceptable use policies of these other networks apply and may limit use.

4. Policy

4.1 General Use and Ownership

4.1.1 The Diocese of Greensburg proprietary information stored on electronic and computing devices whether owned or leased by the diocese, employee or a third party, remains the sole property of the Diocese of Greensburg or its affiliated parishes, schools or Catholic Charities. You must ensure through legal or technical means that proprietary information is protected.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Diocese of Greensburg proprietary information.

4.1.3 You may access, use or share diocesan proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Personal use may be restricted if the resources consumed interfere with utilization of the system(s) for business purposes or if the time spent on Internet resources for personal reasons decreases the employee's productivity.

4.1.5 The Diocese prohibits accessing Internet services that do not further or are contrary to the mission or doctrine of the Church. This specifically includes, but is not limited to, subjects pertaining to pornography.

4.1.6 Users should understand that **all** Internet traffic can be monitored at **all** times.

4.1.7 For security and network maintenance purposes, authorized individuals within the diocese may monitor equipment, systems and network traffic at any time.

4.1.8 Diocese of Greensburg reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must: 1) have all applicable security updates installed 2) anti-malware software shall be used and kept up-to-date 3) firewall software shall be used and kept up-to-date 4) devices shall require authentication via sign-on or login by users 5) devices shall not operate as an

unauthenticated email relay or proxy service and 6) services that are not necessary for the device to perform its function or mission shall be disabled.

4.2.2 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.3 Postings by employees from a diocesan email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the diocese, unless posting is in the course of business duties.

4.2.4 Employees should not open e-mail attachments received from unknown senders, which may contain malware. Contact the sender, if possible, to verify validity of the attachment; otherwise forward the email to the Helpdesk.

4.3 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).

Under no circumstances is an employee of the Diocese of Greensburg or any of its affiliated parishes, schools or Catholic Charities' offices authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing diocesan-owned 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.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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.

2. 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 diocese or the end user does not have an active license is strictly prohibited.

3. Accessing diocesan data, a server or an account for any purpose other than conducting diocesan, school, parish or Catholic Charities' business, even if you have authorized access, is prohibited.

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

5. Using a diocesan, parish or school 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.

6. Making fraudulent offers of products, items, or services originating from any Diocese of Greensburg account.

7. 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. 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.

8. Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technologies team is made.

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

10. Introducing honeypots, honeynets, or similar technology on the Diocese of Greensburg network.

11. 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.

12. Providing information about, or lists of, Diocese of Greensburg employees, contributors, volunteers, parishioners, students or parents to parties outside the Diocese of Greensburg.

4.3.2 Passwords

All personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any diocesan facility, has access to the diocesan network, or stores any non-public diocesan information are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at a minimum of one time per year.

2. Do not share diocesan passwords with anyone, including assistants, secretaries, managers, co-workers while on vacation, and family members. **All employees and some authorized volunteers in the Diocese of Greensburg have their own login to electronic resources. Passwords should not be shared among employees, nor should any employee need to login or be logged in as another user. Additional rights to user resources can be given to any employee via their own login.**
3. In order to provide needed support, IT team members may need to temporarily change an employee's password. After being changed, IT will then send it to the employee, who will be prompted to change it on their first login. This is the only acceptable situation for sending a password digitally.
4. Users must not use the same password for diocesan accounts as for other non-diocesan access (for example, personal email account, option trading, benefits, and so on).
5. Passwords must not be revealed over the phone to anyone.
6. Do not reveal a password on questionnaires or security forms.
7. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption, or device security code lock.
8. Do not use the "Remember Password" feature of applications (for example, web browsers).
9. Any user suspecting that his/her password may have been compromised must report the incident to the Helpdesk and change all passwords.

4.3.3 Email, Social Media, Blogging and Web Communication Activities

When using organization resources to access and use the Internet, users must realize they represent the diocese and all communication activities should be performed in a professional and responsible manner, that don't violate diocesan policy, and that are not detrimental to the diocese's best interests. Please refer to the *Diocesan Electronic Mail Policy, Social Media Policy, Web Content Policy, Pastoral Code of Conduct.* Questions may be addressed to the IT Help Desk.

5. Policy Compliance

5.1 Compliance Measurement

The Information Technologies team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback from stakeholders including the policy owner.

5.2 Review and Update Expectations

This policy will be periodically reviewed and updated by the Director for Information Technology.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

6. Related Policies

- Electronic Mail Policy
- Web Content Policy
- Social Media Policy

7. Definitions and Terms

- Honeypot - Programs that simulate one or more network services accessible on network ports you designate. A honeypot can be used to log access attempts to those ports including the attacker's keystrokes. This could give advanced warning of a more concerted attack.
- Honeynet – one or more honeypots on a network.

8. Revision History

Date of Change	Responsible	Summary of Change
1/26/15	IT Director	Updated and replaced Internet Acceptable Use Policy and replaced, by inclusion, the Software Management Policy