Diocese of Venice
Information Technology
Policy and Procedures

July 22, 2013

Overview and Purpose

This document establishes computer and internet usage guidelines for all entities of the Diocese of Venice. The school and parish entities of the Diocese of Venice provide a wide array of computing, networking, and telecommunications resources and services to their staff. These resources are in place to facilitate teaching, learning, and administrative activities and to further the Diocese of Venice mission. This document contains information technology policies and procedures and also outlines responsibilities of those who use computing and networking facilities at the parishes. Users of these services agree to abide by and be subject to the terms and conditions contained in this and all other applicable policies. Some entities may have additional facilities, practices, and policies that apply to the use of computing facilities in those departments. These policies are designed to enable high quality services and maximize productivity while protecting the rights of all members of our community.

Throughout this document the use of the term **entity** refers to parish and/or school.

Access to Information Technology Resources

Eligibility

Information Technology Resources (computer hardware, software, telephone systems, networks, services, data, and other information) are made available at every parish and parish entity to support and facilitate the administrative functions of those entities and also to help facilitate the research and teaching of the schools and parishes. Access to these resources is provided to the administration, staff, and approved volunteers consistent with their responsibilities. Under no circumstances may anyone use the parish and school IT resources in ways that are illegal (e.g. copyright violations), threaten the entities tax exempt or other status, or interfere with reasonable use by other staff members of the parish and school community. - Other individuals, upon submission of a request, may be granted access to some, or all, of the entities IT resources by the pastor or administrator of that entity. The terms of access will be stated at the time access is granted.

Account Activation/Termination

E-mail access within the entities is controlled through individual accounts and passwords. Each user of the entity's e-mail system is required to read and agree to this E-Mail Acceptable Use Policy prior to receiving an e-mail access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.

Convention for User Names

The standard email naming convention for access to electronic systems comprises the last name, followed by the entity's full domain name. If duplicates occur, the first name initial is generally pre-pended to the last name to resolve ambiguity. Variances of this convention are allowable based on what works best for each entity.

Management of Internet Bandwidth
An entity's network, including the connection to the Internet, is a critical shared resource for supporting administrative needs. Uses of the Internet connection that are central to the operational and administrative mission of the Diocesan entities (e.g. access to DOV web, e−mail, and other sources) will receive higher priority during normal business hours (i.e. critical times). Each entity reserves the right monitor the content of traffic on the network. It is the responsibility of each person using the entities resources, including the network, to do so in an ethical and legal manner. Particular attention should be given to observing copyright laws for digital materials.

Personal Computers on the Network
Internet addresses are assigned dynamically by a DHCP server. In order to obtain a static Internet (TCP/IP) computer address, the owner of the system must register the computer with the entity's IT. The rules and regulations contained in this policy pertaining to electronic mail and Internet access are equally applicable to the use of personal machines for file sharing or as servers. If bandwidth or other problems occur, the entity reserves the right to discontinue access to the machine. Computers connected to the network may not be used as servers for private enterprises, commercial activity, or personal profit. Computers connected to the network may not be used to provide access to the Internet for anyone not formally affiliated with the entity. If personal computers on the entity's network are used as servers, the administrator has the additional responsibility to respond to any use of the server that is in violation of these policies and procedures. Server administrators must take steps to prevent recurrence of such violations and report these violations to the entity's administrator. The entity reserves the right to disconnect any network port whose activity causes an adverse effect on the network or on any other user. Network connections may also be revoked in the case of malicious or inappropriate computing activity on the network.

The entity reserves the right to restrict access to the network during expansion, or for diagnostics and maintenance services. Every effort should be made to provide advance notification and schedule such disruptions during times of minimum impact and traffic.

Virus Protection
The all entities should require that all PC's on their network must have anti−virus software on entity computers. For staff employees, this should be handled automatically by the IT administrator. For non-entity PC's, proof must be provided to the IT administrator before any computer is be permitted on the network.

Printers and Other Peripheral Equipment
Many entities provide networked printing locations throughout their departments. Individual desktop printers, scanners and other peripheral equipment maybe provided at the entity's discretion.

Responsibility for Equipment
Every individual working at the entity is responsible for taking reasonable safety precautions in regard to entity owned computer equipment. Individuals will be held responsible for damage to such equipment arising out of their negligence or intentional misconduct.

Upgrades and Renewal
For computer equipment due to be replaced or needed to be replaced, it will be up to the sole discretion of the entity's administrator or pastor.

Web Posting and Development

Overview:
The accuracy, timeliness, design, and speed (performance) of the web site are of strategic importance to the entity since many external constituents view our web site.

Management of an Entities Web Site
With approval from the entity's administrator or pastor, the webmaster of that entitiy is the policy making body for the development of the presence on the web site. The webmaster and entity administrator/pastor approves the design of the main home page (including the categories/ headings) and style guidelines for individuals/ organizations that wish to contribute to the content of the site. Together, they should approve the linking of new pages to the Web site, rules on policy interpretations, and advises on matters of resource allocations. Given the nature of the World Wide Web (WWW), entity employees cannot operate their own servers.

Procedures
Departments and Diocesan entities can obtain space on the Catholic Center's web site for the development of departmental web pages with the approval of the web site design committee. Any organizations outside the Catholic Center that are not part of the Diocese of Venice may not host their site at the Catholic Center.

Content Management administration is handled specifically by the web site design team. Any Content updates for the web site needs to be forwarded to the entity's department head for review and approval before it will be added to the web site.

Copyright and Links to Commercial Organizations
The use of an entities Web site must be consistent with other Diocesan policies relating to use of information technology resources. Of particular note are the restrictions on the use of copyrighted material and the use of external resources for profit−making activities. Placing copyrighted material on the Web site without permission of the author is prohibited. Links to organizations outside the diocese or entity, that appear on the Catholic Centers or entity's departmental or organizational Web pages must be directly related to the stated mission of that department or organization. These links should not infer a preference for a particular organization, but rather should be informative of the range of options available to those who might need the information provided by these links. Links from any catholic or charitable web pages that generate income to a department, organization, or individual might compromise the Diocesan entity's tax exempt status, and as such are prohibited.

Hardware Standards
Guidelines for standards are based on the current technology available combined with the current needs of its user today. These apply to both the Macintosh and Linux platforms. The primary considerations for each configuration (desktop, printing, portable computing) are:
Ease of connectivity to the network

1. Consistent performance of all integrated components in our network environment;
2. Industry leader with an established track record in manufacturing, reliability and service;
3. Successful in house experience with the chosen product and configuration
4. Serviceability
5. The machine has a minimum MTBF lifetime of four years

Software Standards Goals Moving Forward

Rationale:
In a networked environment, the ability to easily share information is important. Ideally, the ease of sharing should not depend upon which hardware environment is being used on the desktop (Windows or Macintosh). Central to making sharing facile is the entity's IT department, particularly software used for word processing, spreadsheets, databases, network browsing, and electronic mail. The following are advantages of entity wide software standards:

Improved Data Sharing
Consistency of file formats provides for optimal file sharing capabilities between individuals, departments, and groups across the entity campus. Identical resources on each desktop (private offices and public labs) provide ease of transferability and a consistent tool set for all users, from any area will be available. Sharing of data between applications (word processors, spreadsheets, and data bases) is seamless. Simplified Budgeting and Purchasing Software standards would permit centralized budgeting and purchasing. This would relieve an individual or department from the time consuming tasks of choosing a product, tracking down the best pricing and product availability, and generating the proper paperwork to place an order for the product. Significant savings can be achieved through site licenses or quantity discounts and utilizing Open Source Software.

Improved Support
IT support personnel can focus on depth of application knowledge rather than breadth of numerous applications. Product expertise means questions can be answered quickly and efficiently. Support efforts can be focused on supporting the end user and documenting known problems. Support could come from any member of the entity's IT department, since most will be using or should be somewhat familiar with the application.

Improved Training
Training teams can be established to focus on developing curricula for levels of user proficiency (introductory, intermediate, and advanced). Training consultants from outside the entity can be used more effectively and economically. Smoother Software Installation and Upgrades Software installations for new machines should become invisible to the end users by making it part of the hardware installation. Installations can become routine, rather than a specialized process for each individual, resulting in time savings. Installations and

upgrades should be made available to all users via the network, and automated for consistency. Upgrades can be tested and documented prior to center wide deployment to reduce potential incompatibility problems. Simplified Software Licensing Separate record keeping for software licenses would not be required by the individual; rather it could become part of the central inventory of hardware.

Software Standards:
Microsoft Word
Microsoft Excel
Microsoft PowerPoint
Microsoft Outlook
Microsoft Publisher
Internet Explorer
Adobe Acrobat Creator/Reader
Logos
Quickbooks (cloud based)

Telephone and Voicemail Acceptable Use Policy

Purpose
Telephone communication is an essential part of the day-to-day operations. Telephone and voicemail services are provided to employees in order to facilitate the day to day activities. The goal of this policy is to balance the business need for telephone and voicemail with the costs involved. Appropriate common sense should be used when making long distance and international calls since entities incur additional service provider fees from external sources.

Scope
This policy applies to all employees of Diocese of Venice and its entites, and all usage an entity's telephone and voicemail services.

Basic Policy
The use of telephones and voicemail should be as cost effectively as possible and in keeping with the best interests of all Diocesan entities. All employees should operate within the following basic policy guidelines. Further information on appropriate and inappropriate use follows this section.

 All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of the Diocesan entity.

 The Diocesan entity is responsible for installation and repair of all telephony equipment and administration of telephone and voicemail accounts.

 Department supervisors are responsible for overseeing telephone and voicemail use and ensuring policy compliance, as well as ensuring the administrator/pastor is notified of any adds, moves, or changes required to telephone or voicemail services.

 All employees are eligible to receive a telephone based on their needs and at the discretion of the administrator/pastor.

 All voicemail boxes will be protected with a password. Passwords must not be shared with others.

 A voicemail box can hold several minutes of message storage time. If a voicemail box is full, no further messages can be recorded. Read voicemail messages will be up to the employee to delete after 90 days. Voicemails can also be forwarded as an email attachment if desired.

 Use of directory assistance (i.e. 411) should be avoided since a fee is incurred with each use. If you are unsure of a number, please consult print or online telephone directories first.

Unacceptable Use
An entity's telephone and voicemail services may not be used for the following:

 Transmitting obscene, profane, or offensive messages.

 Transmitting messages or jokes that violate our harassment policy or create an intimidating or hostile work environment.

 Using the telephone system or breaking into a voicemail box via unauthorized use of a password.

 Broadcasting unsolicited personal views on social, political, or other non-business related matters.

 Soliciting to buy or sell goods or services unrelated to the entity.

 Calling 1-900 phone numbers.

 Making personal long-distance phone calls without supervisor permission.

Misuse of telephone and voicemail services can result in disciplinary action, up to and including termination.

Limited Personal Acceptable Use

In general, personal use of telephone and voicemail services is allowable, but must be limited in number and duration and must not interfere with performance of official business duties. Limited personal acceptable use is allowed under the following circumstances:

 An employee's work schedule changes without advance notice and the employee must notify a family member or make alternate transportation or childcare arrangements.

 Brief local calls to a spouse, minor child, or elderly parent, or to those responsible for them (e.g. school, daycare center, nursing home).

 The employee needs to make a call that can only be made during regular working hours, such as to a doctor or local government agency.

 The employee needs to make arrangements for emergency repairs to his or her residence or automobile.

 A call that reasonably could not be made at another time and is of moderate duration.

Any personal long-distance calls that must be made (excepting toll-free 1-800 calls) should be charged to the employee's home telephone number, personal credit card, personal calling card, or be charged to the called party. If a personal long-distance call must be made that will be billed to the entity, the employee should receive permission from a supervisor to make the call first. Regardless, employees are expected to reimburse center for the cost of any long-distance calls within a reasonable timeframe of receipt of the relevant bill.

Monitoring

The Diocesan entity reserves the right to monitor telephone and voicemail use, including telephone conversations and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as to retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts.

 Date, time, length of call, number called;

 Costs per call;

 And type of usage.

Service and Repair
If there is a problem with an existing telephone or voicemail box, contact the entity's IT administrator to assist in resolving the issu.

Telephone Procedures
All employees that receive a telephone also receive the manual on how to operate their phone. It is the employee's responsibility to learn how to operate their phone. For any substantial changes to the phone system, training should be provided as required.

Voicemail Procedures
All employees are to follow the entity's voicemail phone system procedure. How to setup your voicemail should be in the manual you received with your telephone if applicable. If you have trouble setting up your voicemail, you should contact the IT person for help.

Printer Policy

Purpose
Printers represent one of the highest equipment expenditures at an entity. The goal of this policy is to facilitate the appropriate and responsible business use of the entity's high end printer assets, as well as control printer cost of ownership by preventing the waste of paper, toner, ink, and so on.

Scope
This Printer Policy applies to all employees, as well as any contract employees who may be using the entity's network and equipment.

General Recommend Policy

1. Printers are to be used for documents that are relevant to the day-to-day conduct of the entity's business. Printers should not be used to print personal documents.

2. Installation of personal printers is generally not condoned. However, in certain circumstances, where confidentiality, remote location, the need to print a large number of low volume print jobs, or other unusual situation is an issue, personal printers may be allowed.

3. If you print something, please pick it up in a timely fashion. If you no longer want it, please dispose of it appropriately.

4. If you come across an unclaimed print job, please stack it neatly and turn into the main office.

5. Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers and other optimization features (e.g. printing multiple PowerPoint slides per page versus only one per page for draft purposes).

6. Make efforts to limit toner use by selecting light toner and lower dpi default print settings.

7. Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer.

8. If printing a job in excess of 25 pages, please be at the printer to collect it when it comes out to ensure adequate paper supply for the job and that the output tray is not overfull (i.e. you may need to remove some of the output before the print job is finished).

9. Avoid printing e-mail messages. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.

10. Avoiding printing a document just to see what it looks like. Use the print preview option on your computer.

11. Avoid re-using paper in laser printers, as this can lead to paper jams and other problems with the machine.

12. Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with someone knowledgeable to find out which machine can handle these specialty print jobs.

13. Color printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) will do.

14. Printer paper and toner should be stocked at all machines

15. If you encounter a physical problem with the printer (paper jam, out of toner, etc.) and are not "trained" in how to fix the problem, please do not try. Instead, report the problem or ask a trained co-worker for help.

16. Report any malfunction of any printing device to person responsible for getting it repaired.

Wireless Security Access Policy and Agreement

Purpose
The purpose of this policy is to define standards, procedures, and restrictions for connecting to an entity's internal network(s) or related technology resources via any means involving wireless technology. This can include, but is not limited to, access from the following:

 External hosts via remote access technology (for example, using a wireless router at home to connect to the entity's Virtual Private Network).

 Wireless gateways on the entity's premises.

 Third-party wireless Internet service providers (also known as "hotspots").

The policy applies to any equipment used to access internal networked resources, even if said equipment is not entity, owned, or supplied. For example, use of a public library's wireless network to access the entity's network would fall under the scope of this policy. The overriding goal of this policy is to protect the entity's technology-based resources (such as data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of funds, and damage to our public image. Therefore, all users employing wireless methods for accessing the entity's technology resources must adhere to diocesan-defined processes for doing so.

Scope
This policy applies to all Diocesan entity employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize Diocesan entity owned, personally-

owned, or publicly-accessible computers to access the organization's data and networks via wireless means. Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment at any Diocesan entity does not automatically guarantee the granting of wireless access privileges. Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are to be used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organizational data. Addition of new wireless access points within the entity's facility will be managed by an entity employed and knowledgeable person. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the Diocesan entity's network, is strictly forbidden. This policy is complementary to any previously-implemented policies dealing specifically with network access and remote access to the enterprise network.

Supported Technology

All wireless access points should be firewalled and be centrally managed by the Entity's IT person and should utilize WPA encryption, strong authentication, and other security methods at the entity's discretion. Users are expected to adhere to the same security protocols while utilizing entity equipment on a public WiFi network. Failure to do so could result in immediate suspension of all network access privileges so as to protect the entity's infrastructure.

Eligible Users

All employees requiring the use of wireless access for business purposes must contact their IT department or person to gain access to the wireless network.

Employees may use privately owned connections for business purposes. If this is the case, the entity's IT person must approve the wireless connection as being secure and protected. However, the entity should not support third-party wireless hardware or software, a hotspot wireless ISP connection, or any other wireless resource located outside the entity's firewall .

Policy and Appropriate Use

It is the responsibility of any employee of a Diocesan entity who is connecting to the organizational network via wireless means to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that any wireless connection used to conduct Diocesan business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user"s account. Based on this, the following rules must be observed:

1. General access to the organizational network through the Internet by residential remote users through the Diocesan entity's network is permitted. However, the employee should not use the Internet for recreational purposes.

2. Employees using wireless access methods will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with the Diocese password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

3. All remote computer equipment and devices used for business interests, whether personal- or entity owned, must utilize reasonable physical security measures. Users are expected to secure their connected machines when they are physically at their machines, as well as when they step away. Computers will have installed whatever antivirus software deemed necessary by the entity's administration. Antivirus signature files must be updated in accordance with existing Diocesan IT policy.

4. Due to the potential for bandwidth conflicts within the entity's network, use of unsanctioned equipment operating within the 2.4 GHz range is strictly forbidden. If you have a need to use such equipment – for example, a wireless phone – please consult with the entity's IT person before proceeding further.

5. Prior to initial use for connecting to the entity's vpn network, all public hotspots should be registered.

6. Remote users using public hotspots for wireless Internet access must employ for their devices an approved personal firewall, VPN, and any other security measure deemed necessary. VPNs supplied by the wireless service provider should also be used, but only in conjunction with the entity's security measures. The entity may approve, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product. Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, war drivers, and eavesdroppers.

7. Any remote connection (i.e. hotspot, ISDN, frame relay, etc.) that is configured to access the entity's resources must adhere to the authentication requirements of the Diocese's IT Department. In addition, all hardware security configurations (personal or entity owned) must be approved by the entity.

8. Employees, contractors, and temporary staff will make no modifications of any kind to entity owned and installed wireless hardware or software without the express approval of the entity's administration.

9. Employees, contractors, and temporary staff with wireless access privileges must ensure that their computers are not connected to any other network while connected to the entity's network via remote access.

10. The wireless access user agrees to immediately report to his/her manager, any incident or suspected incidents of unauthorized access and/or disclosure of entity resources, databases, networks, and any other related components of the organization's technology infrastructure.

11. The wireless access user also agrees to and accepts that his or her access and/or connection to entity's networks may be monitored to record dates, times, duration of access, data types and volumes, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

12. The entity reserves the right to turn off without notice any access point to the network that puts the entity's systems, data, users, and affiliates at risk.

Policy Non-Compliance
Failure to comply with the Wireless Security Access Policy and Agreement may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

Web Posting Policy

Purpose
The Catholic Center maintains a Web site to provide information about the Diocese of Venice to the South Florida Catholic community and the public at large. Individuals, departments, divisions, and parishes may develop and maintain local Web pages within the dioceseofvenice.org domain but only by approval of the Catholic Center's Communications Department. These guidelines are to insure that Web pages within the dioceseofvenice.org domain further the purpose of the Catholic Center's Web site.

Content Guidelines
The object of these guidelines is to ensure that the content of Web pages accurately represent the Catholic Center.

1. Content must be consistent with the purpose of the Catholic Center's Web site.

2. Content must conform to Acceptable Use Policies and the Catholic Center's Web Policy so that it is

- Non-discriminatory,

- Non-commercial, and

- Protective of individual privacy.

3. Language must be suitable to a public forum.

4. Content provided must be appropriately current and accurate.

5. Links are to be monitored, with non-functioning links removed or repaired regularly.

Format Guidelines
The object of these guidelines is to ensure that Web pages present a favorable, professional image of the Catholic Center's.

1. Spelling and grammar should be correct.

2. HTML should be used correctly.

3. Use of the the Catholic Center's logo should comply with the the Catholic Center's banner

4. Images should load correctly within a reasonable amount of time.

5. Relative links should be used in place of the full URL whenever possible.

6. Navigational aids should be provided to assist the user in returning to the Catholic Center's home page or the user's page should open in a new page.

7. Documentation should be displayed on each page to indicate:

- Person or office responsible for the page,

- E-mail address or phone number of individual to contact about page, and

- Date page was last updated. To avoid confusion with different international date conventions, spell out the month (e.g. February 11, 1999 or 11 FEB 99 rather than 02/11/99).

8. Institutional and local pages should include information to facilitate accurate indexing by search engines.

9. Pages should be checked before posting.

- Examine pages with recent versions of Firefox 3.0 and Internet Explorer Version 8.0.

- HTML Code Checking: W3C's HTML Validation Service

All Web content submitted must be approved prior to posting. All submissions must be entered at least two days in advance of the requested posting date. If significant changes are required to the content, this timeframe may be extended.

Submission of Copyrighted Work

No employee of a Diocesan entity may reproduce any copyrighted work in violation of the law. Copyrighted works include, but are not limited to: text (e.g. articles), images (e.g. photographs), graphics (e.g. logos), sound recordings (e.g. MP3s), video recordings (e.g. movies), or software programs. In some countries, such as the U.S., copyrighted materials are not required by law to be registered, unlike patents and trademarks, and may not be required to carry the copyright symbol (©). Therefore, a copyrighted work may not be immediately recognizable. Assume material is copyrighted until proven otherwise. If a work is copyrighted, you must seek out and receive express written permission of the copyright holder to reproduce the copyrighted work in order to avoid violation. This also includes all copyrighted works held by the entity.

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

Network Security Policy for Portable Computers

Introduction
Portable computers offer staff the ability to be more productive while on the move. They offer greater flexibility in where and when staff can work and access information, including information on the entity's network. However, network-enabled portable computers also pose the risk of data theft and unauthorized access to the entity's network. Any device that can access the entity's network must be considered part of that network and therefore subject to policies intended to protect the network from harm. Any portable computer that is proposed for network connection must be approved and certified by the entity.

Protecting the Laptop
In order to qualify for access to an entity's network, the laptop must meet the following conditions: Network settings, including settings for our VPN, must be reviewed and approved by IT support personnel. A personal firewall must be installed on the computer and must always be active. Anti-virus software must be installed. Software must have active scanning and be kept up-to-date.

Laptop User's Responsibilities
The user of the laptop is responsible for network security of the laptop whether they are onsite, at home, or on the road. The user of the laptop is responsible for keeping their anti-virus scanning software up-to-date at all times. It is strongly recommended that they update

their anti-virus software before going on the road. The user of the laptop shall access network resources via a VPN connection. Use of public Internet services is discouraged, as they do not offer adequate protection for the user.

Security Audits
The Diocesan's IT Department reserves the right to audit any laptop used for Diocese of Venice business to ensure that it continues to conform to this certification policy. The IT Department will reserve the right to deny network access to any laptop which has not been properly configured and certified.

Anti-Virus Policy

Purpose
A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to an entity in terms of lost data, lost staff productivity, and/or lost reputation. As a result, one of the goals of the Diocese of Venice IT department is to provide a computing network that is virus-free for all entities. The purpose of this policy is to provide instructions on measures that must be taken by all Diocesan employees and staff to help achieve effective virus detection and prevention.

Scope
This policy applies to all computers that are connected to an entity's network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both Diocesan entity-owned computers and personally owned computers attached to the entity's network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

General Policy
It is strongly recommend and required that all entities utilize approved anti-virus software. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date. Any activities with the intention to create and/or distribute malicious programs onto the entity's network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the entity's IT Department immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT Department.

Any virus-infected computer will be removed from the network until it is verified as virus-free.

Rules for Virus Prevention

Always run the standard anti-virus software provided by your entity. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media. Avoid direct disk sharing with read/write access. Always scan a floppy diskette for viruses before using it. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder. Back up critical data and systems configurations on a regular basis and store backups in a safe place. Regularly update virus protection on personally owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

IT Department Responsibilities

The following activities should be the responsibility of an entity's IT Department or IT support person: The IT Department is responsible for maintaining and updating this Anti-Virus Policy. The IT Department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use. The IT Department will apply any updates to the services it provides that are required to defend against threats from viruses. The IT Department will install anti-virus software on all entity owned and installed desktop workstations, laptops, servers, tablets and smart phones.

The IT Department should be available to assist employees in installing anti-virus software according to standards on personally owned computers that will be used for business purposes.

The IT Department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT Department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network. The IT Department will perform regular anti-virus sweeps. The IT Department will attempt to notify users of the entity's system of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

Administrative Responsibilities for Entity Owned IT Property

The office management for each Diocesan entity is responsible for assigning a liaison to ensure that the technology (software and hardware) is being properly managed and secured. For entities that do not have qualified personnel that can be assigned to handle IT properties, the Diocese of Venice IT department should be notified so that proper precautions can be taken to protect and secure the entities IT infrastructure.

Specific areas that need to be secured & managed include the following;

Password assignments which should be kept updated and filed in a secure location so that access by qualified and designated personnel can gain access when required.

System maintenance and warranty records should be kept on file for each computer owned by the entity.

Nightly backups should be monitored on ongoing bases with backups being stored off-site where ever possible.

All computers should be password protected and either shut down or screen locked using password protection when the computer will be left alone for an extended period of time. Passwords should be changed every 60 – 90 days and should not be reused.

Server rooms and server closets should be kept secured at all times.

Remote access should only be allowed by qualified personnel.

All applications (where applicable) and computers should be password protected with strong password. See policy on password conventions. This must be enforced by office management.

Department and Individual Responsibilities
The following activities are the responsibility of all IT support personnel and employees: Departments must ensure that all departmentally managed computers have virus protection that is in keeping with the standards set out in this policy. Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy. All employees are responsible for taking reasonable measures to protect against virus infection. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to their entity's network without the express consent of the entity.

Enforcement
Any employee who is found to have violated this policy is subject to the Employee Conduct Code and may be subject to disciplinary action, up to and including termination of employment.