



# **Catholic Archdiocese of Atlanta**

## **Information Systems**

### **Parish Minimum Network Security Requirements**

**6.8.2006**

**Tom Pope**  
**Director of Information Technology**  
**Catholic Archdiocese of Atlanta**

## **Reason for Security Requirements**

### **Access to Information Resources**

The Catholic Archdiocese of Atlanta is providing access to information and information technology resources to facilitate normal business activities for all parishes of the Catholic Archdiocese of Atlanta while at the same time reducing exposure to unauthorized access of both employees and non-employees.

With the rollout of centralized applications like Parishsoft, LOGOS and HR Online, many of Catholic Archdiocese of Atlanta parishes rely or will rely on information technology to perform their job functions.

Access to information resources should be reasonably simple, have integrity and maintain confidentiality. While security measures can sometimes complicate legitimate access, the consequences of security problems that result from unauthorized access can be severe. The Catholic Archdiocese of Atlanta and all parishes must work collectively to ensure that all systems meet basic security requirements.

The standards provided below are the minimum requirements. Parishes are encouraged to provide enhanced security if required or desired.

### **Basic Computer Security**

Require passwords

Require reasonably complex passwords (no blank passwords)

Require & enforce periodic password changes

Do not share passwords or logins

Do not document passwords

Logout or shutdown computers when leaving for the day

Enforce screen savers with password protection

    5 minute screen saver activation timeout in common or public areas

    30 minute screen saver activation timeout elsewhere

Ensure that local PC antivirus subscriptions are active and up to date

Turn on Automatic Updates on Windows XP/2000 machines

No Windows 95, 98 or ME systems

## **Networks**

### Hardware Based Firewall

Cisco PIX, Sonicwall, Linksys, etc.

Software based firewalls are discouraged.

The Microsoft ISA firewall is not permitted because of functional conflicts with Parishsoft.

### Fast Ethernet or better switches

Hubs are discouraged because of their 'broadcasting' method of communication.

Switches provide improved function and performance.

### Remote Access

Access to the parish network from outside the firewall should only be allowed to those who require access to meet our business needs. Such access must be monitored and passwords changed periodically. All remote access should be controlled by the firewall.

## **Wireless Networks**

### WPA Wireless Security - Wi-Fi Protected Access

Minimum WPA Encryption (may require hardware upgrades).

WEP (Wired Equivalent Privacy) has been exploited and should be avoided if possible.

### No 'Hot Spots'

No 'open' systems that do not require authentication, encryption or reasonable security.

These are similar to coffee shops that allow anyone to connect to the system. 'Hot Spots' are large security holes easily exploited by the technically knowledgeable or malicious software.

## **Server environment**

### Windows 2000 Server (or better)

Windows 2003 Standard is the recommended operating system (OS) in server environments. It is widely supported and, when properly installed, patched and maintained, is sufficiently secure.

### Windows 2000 Active Directory

Windows 2000 / 2003 uses a centralized database called 'Active Directory' to provide secure access to various resources (printers, files, etc) on the network. Users can be created and limited to specific resources using tools built into Active Directory.

### Centralized Antivirus

When in a server environment, centralized antivirus is ideal to enhance local system health. Updates can be centrally obtained, monitored and distributed. Products like Symantec Antivirus Corporate Edition allow for a central repository for infected files and can be configured to automatically correct or delete the suspect file or files.

## **Workstations**

### Windows 2000 or XP operating systems – No Windows 95, 98 or ME

Windows 95, 98 or ME have no built-in security and are easily breached. Computers with these older operating systems must be upgraded or replaced.

### Turn on Automatic Updates

Microsoft provides a tool for ensuring that weaknesses found in its operating systems and products are easily corrected. The tool, Automatic Updates, can be scheduled or can be manually run.

### Antivirus software should be current

Ensure that the antivirus subscriptions are active and up to date. Most 'consumer grade' antivirus products now include scanning of adware, spyware and malware as well as spam filtering. These can be tricky to setup but once properly configured are an excellent layer of security.

The following is not required but recommended.

## **Basic Workstation Hardware Recommendations**

### Pentium 4 or similar speed processor

Pentium 4 processors or better are HIGHLY recommended. The applications being rolled out by the Archdiocese require higher processing power than older units can adequately provide.

### RAM – 512 MB or Better

The single best performance enhancing upgrade to a PC is to increase its RAM memory. On new units, 1 GB of RAM is recommended.

### LCD Monitors

Although not a performance enhancement, LCD screens are easier on the eyes and take up less desk space.

If you have any questions regarding this document, please feel free to contact the Archdiocesan Information Technology department Director, Tom Pope @ 404.885.7432 or email at [tpope@archatl.com](mailto:tpope@archatl.com).