PRINCE GEORGE'S COUNTY, MARYLAND
FIRE/EMERGENCY MEDICAL SERVICES DEPARTMENT GENERAL ORDER

General Order Number: 03-06	**Effective Date:** January 2010
Division: Communication and Information Management/Technology	
Chapter: Information Management Policies and Procedures Manual	
By Order of the Fire Chief: Marc S. Bashoor	**Revision Date:** N/A

POLICY

This General Order establishes the Information Management Policies and Procedure Manual to ensure that personnel are familiar with the Information Management functional area of the Department as it relates to information management and information technology.

DEFINITIONS

See Terms and Definitions in the Policies and Procedure Manual

PROCEDURES / RESPONSIBILITIES

1. Introduction

Information Management (IM) is responsible for the development, implementation, and administration of policies and procedures to ensure the integrity, confidentiality, and availability of the Department's data resources and automated system components.

Information Management also maintains a working relationship with the County's Office of Information Technology and Communication (OITC). OITC is the centralized support agency responsible for the innovation, implementation and advancement of technologies in Prince George's County Government. Personnel in OITC assist IM personnel in maintaining various computers and peripherals, software applications, and ensuring that the County's computer network is operational as close to 100% of the time as possible.

2. Duties and Responsibilities

Information Management integrates information standards, process systems and technology to enable the exchange of information among providers and users in order to support the management objective of the Fire/EMS Department. Designated as the "Help Desk" for the Fire/EMS Department for troubleshooting computer problems, Information Management supports all fire stations and administrative offices. IM provides technical support, training on the use of hardware and software applications to all Department personnel. This includes over 700 computers, peripherals, and cell phones.

Information Management serves as the Custodian of Records for the Fire/EMS Department. As Custodian of records Information Management:

- Maintains and stores confidential Fire and EMS reports

- Reviews Maryland Ambulance Information System (MAIS) reports for submittal to the Maryland Institute for Emergency Medical Services Systems
- Ensures that the Fire Records Management System is up to date in order to submit incident information to the Maryland Office of the State Fire Marshal
- Processes requests for information and reports for the public, the Department, other agencies, and the media per the Freedom of Information Act (FOIA)
- Answers and coordinates information released in response to subpoenas for the State and County government

Additionally, the IM team provides Fire and EMS statistics for management, the public, other fire departments and governmental agencies. As such Information Management maintains an up to date records management system and ensures that adequate computer related training programs and computer systems are in place.

Other duties and responsibilities include:

- Maintaining, analyzing, troubleshooting, and repairing computer systems, hardware and computer peripherals.
- Documenting and maintaining upgrades or replacing hardware/software systems where applicable.
- Supporting and maintaining user network and account information.
- Assisting personnel with creating databases and presentations.
- Maintaining the standards set by the Health Insurance Portability and Accountability Act (HIPPA); that gives patients greater control of their health records while setting boundaries on the use and release of health records.

3. Governance

Many of the duties and responsibilities of Information Management personnel are governed by:

- Prince George's County Code, Subtitle 11, Section 11-156
- The Code of Maryland Regulations (COMAR) 30:03:04:04
- The Annotated Code of Maryland Article 38A § 45C(b)(2)
- 45 The Code of Federal Regulations (CFR) 164.502 (d)

The purpose of the Policies and Procedures manual is to ensure that Department personnel are familiar with the policies and procedures set forth by Information Management as it relates to information management and information technology.

Your cooperation is appreciated in ensuring that this process goes smoothly. Personnel from Information Management are available to assist station personnel with the transition of this process. They can be reached at 301-883-7181.

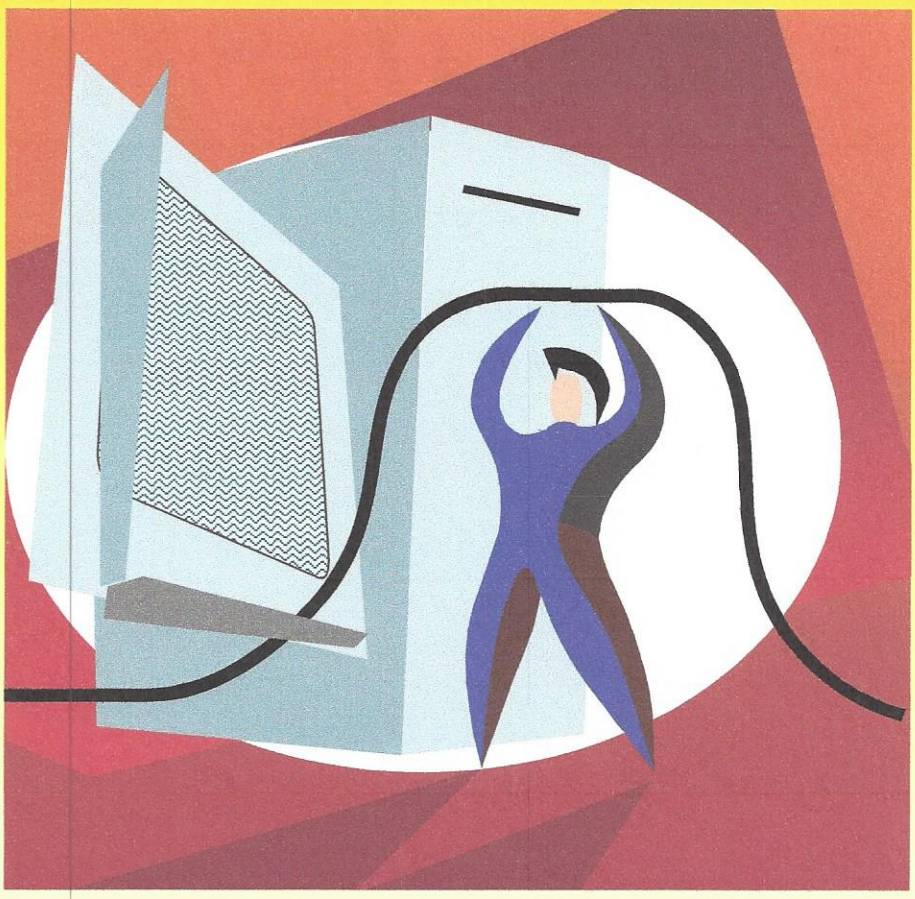
REFERENCES

N/A

FORMS / ATTACHMENTS

Policies and Procedure Manual

Information Management
Policies & Procedures Manual



PRINCE GEORGE'S COUNTY
FIRE/EMS

Effective March 2009

INFORMATION MANAGEMENT

Contact Information
(301) 883-7183
8:30am – 5:00pm
Monday - Friday

Operations Center
(301) 583-2200
After 5:00pm
Weekends and Holidays

TABLE OF CONTENTS

1.0 Prince Georges County Fire/EMS Department Information Management

1.1 Introduction

The Prince George's Fire/EMS Department's Information Management Division (IMD) is responsible for the development, implementation, and administration of policies and procedures to ensure the integrity, confidentiality, and availability of the Department's data resources and automated system components.

Information Management also maintains a working relationship with the County's Office of Information Technology and Communication (OITC). OITC is the centralized support agency responsible for the innovation, implementation and advancement of technologies in Prince Georges County Government. Personnel in OITC assist IMD personnel in maintaining various computers and peripherals, software applications, and ensuring that the County's computer network is operational as close to 100% of the time as possible.

1.2 Duties and Responsibilities

Information Management integrates information standards, process systems and technology to enable the exchange of information among providers and users in order to support the management objective of the Fire/EMS Department. Designated as the "Help Desk" for the Fire/EMS Department for troubleshooting computer problems, Information Management supports all fire stations and administrative offices. IMD provides technical support, training on the use of hardware and software applications to all Department personnel. This includes over 700 computers, peripherals, and cell phones.

The Information Management Division serves as the Custodian of Records for the Fire/EMS Department. As Custodian of records Information Management:

- Maintains and stores confidential Fire and EMS reports
- Reviews Maryland Ambulance Information System (MAIS) reports for submittal to the Maryland Institute for Emergency Medical Services Systems
- Ensures that the Fire Records Management System is up to date in order to submit incident information to the Maryland Office of the State Fire Marshal
- Processes requests for information and reports for the public, the Department, other agencies, and the media per the Freedom of Information Act (FOIA)
- Answers and coordinates information released in response to subpoenas for the State and County government

Additionally, the IMD team provides Fire and EMS statistics for management, the public, other fire departments and governmental agencies. As such Information Management maintains an up to date records management system and ensures that adequate computer related training programs and computer systems are in place.

Other duties and responsibilities include:

- Maintaining, analyzing, troubleshooting, and repairing computer systems, hardware and computer peripherals.
- Documenting and maintaining upgrades or replacing hardware/software systems where applicable.
- Supporting and maintaining user network and account information.
- Assisting personnel with creating databases and presentations.
- Maintaining the standards set by the Health Insurance Portability and Accountability Act (HIPPA); that gives patients greater control of their health records while setting boundaries on the use and release of health records.

1.3 Governance

Many of the duties and responsibilities of Information Management personnel are governed by:

- Prince George's County Code, Subtitle 11, Section 11-156
- The Code of Maryland Regulations (COMAR) 30:03:04:04
- The Annotated Code of Maryland Article 38A § 45C(b)(2)
- 45 The Code of Federal Regulations (CFR) 164.502 (d)

The purpose of this manual is to ensure that Department personnel are familiar with the policies and procedures set forth by Information Management as it relates to information management and information technology.

2.0 TERMS AND DEFINITIONS

Active X - Gives functionality to embedded applications Active X expands various multi media content to view audio, video and animation.

Air Card – A computer device packaged in a small card about the size of a credit card and conforming to the PCMCIA standard. It provides access to a computer network and the internet.

Bandwidth – The amount of data that can be transmitted in a fixed about of time. A rate of data transfer measured in seconds.

Barcode – A machine readable representation of data.

Computer Aided Dispatch (CAD) – A computer system that assists 911 operators and dispatch personnel in handling and prioritizing calls. Enhanced 911 will send the location of the call to the CAD system that will automatically display the address of the 911 caller on a screen in front of the operator. Complaint information is then entered into the computer and is easily retrievable.

Cartridge – A module to be inserted into a larger piece or equipment such as printers for functionality in printing.

Citrix – A server solution that uses Microsoft's Terminals Software applications for computers specializing in remote accessing of applications over a network.

Client – A application that typically runs on a computer or workstation and relies on a server to perform operations.

Communication Box – Casing used to house electronic equipment.

Computer Image – A copy of all programs stored in a computer network folder to be used for restoring and repairing a configuration.

Configuration – The way a system is set-up or the assortment of components that make up a system. A choice of hardware/software and documentation that functions collectively.

Contacts - A collection of screen names in an instant messaging or e-mail program or online game or mobile phone.

CPU – Central Processing Unit, an electronic circuit that executes computer commands and runs programs.

Custodian of Records – A person designated to be responsible for an organization's records and files and ensures that they are kept in compliance with the terms of various regulatory codes and retention schedules.

Data – A collection of facts within a computer. Distinct pieces of information usually formatted in a special way. All software is divided into two general categories 1) data and 2) programs. Programs are collections of instructions for manipulating data.

Domain – A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains are defined by the IP address. All devices sharing a common part of IP address are in the same domain.

Ethernet Cable – A network cable terminated with an RJ45 and used for connecting a computer to the network.

Fire Wall – An integrated security measure to prevent unauthorized electronic access to a networked computer. A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

Flash Player – A software package for creating, viewing animations and movies via a web browser.

Global Address Listing (GAL) –uses a directory service that works with Microsoft's email system. The GAL contains information for all email users.

Helpdesk – A resource center for assisting with technical computer and network problems and concerns.

Home Directory – A file system that contains personal files used on a network.

Hyper Text Transfer Protocol (HTTP) – The protocol used by the server and your computer to transfer the data between them. It also enables Web browsing.

Icons – A small pictogram or picture on a computer desktop the gives direct access to what it represents.

Internet - A global network of interconnected computers enabling users to share information along multiple channels.

Intranet – A private computer network that uses internet technologies to securely share any part of an organizations information or operational system.

Internet Protocol Address (IP) – A numeric address that is given to computers and users connected to a network. An IP address takes the form of four numbers separated by dots, for example: 172.20.18.135. Every machine that is on the Network has a unique IP.

If a machine does not have an IP address, it cannot be on a Network.

JAVA – A computer programming language. Java is an object oriented language similar to C++ but simplified to eliminate language features that cause common programming errors.

JPEG – Joint Photographic Expert Group – Stores images on a computer in a compressed format.

Jump Drive – A detachable digital storage device that carries data and Files.

Keyboard – A set of alphanumeric and command keys used to input information to a computer.

Local Area Network (LAN) – A local area network is a computer network limited to the immediate area, usually the same building or floor of a building LANs are capable of transmitting data at very fast rates, much faster than the data that is transmitted to you over the Internet. A LAN is a collected group of computers linked together by an enclosed network.

Memory – Internal storage area in the computer, Mental ability to store, retain and recall information.

Modem – Transmits decoded analog signals and reproduces it to digital.

Monitor - Visual display unit, a device that displays images.

Network – A group of stations or offices connected by computers, telephones or other devices. Connection can be permanent via cabling, or temporary through telephone or other communications links. The transmission or connection can be physical (ie fiber optic cable) or wireless (ie satellite). A computer network is a data communications system which interconnects computer systems at various different sites. A network may be composed of any combination of LANs or WANs.

Motherboard – The primary circuit in any electronic device or system.

Mouse – A pointing device.

Octet – One of the four number groups in an IP address, for example: in the IP address 172.20.18.135, the third Octet would be the number 18 counting from the left of the IP address.

Packets – The form in which data is passed over a network. Essentially, packets are pieces of a 'big picture'. A complete file, for example is broken into packets, sent to another machine and then reassembled by that machine back into a complete file.

PDF – Portable Document File, a file format created by Abode the includes, text, fonts and images.

Port – An interface on a computer to which a device can be connected. Devices can be printers, keyboards, disk drives, monitors, etc.

Pre Alerting System – An electronic system that runs off the CAD system that alerts station personnel about an emergency incident.

Profile – The computers representation of user information.

Projector – A device that projects a video signal.

RAM – Random Access Memory, the computers memory that can read from and write to.

Resolution – An adjustable level of clarity on a display device such as a monitor.

RJ – Registered Jack (voice or data)

RMS – Records Management System a "record store" used to store data, and allows the user to query, sort, and filter data elements.

Router – A device designed to forwarding data packets along a network.

Security – In the computer industry, security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Server – A computer or device on a network that manages network resources.

Service Tag Number – The number the represents a device for service.

Shared Drive – Access to public areas and disk on a network.

Storage Device – Used for storing data on devices such as disk, jump drives and tape.

Telestaff – A computer software application that primarily functions as a scheduling tool that grants access both remotely and directly to the server.

Thin Client – A Smaller or Slim computer which runs off a remote server and grants access to a network.

Transmission Control Protocol (TCP) – A protocol used along with IP to send data in

the form of individual units between computers over the Internet. Whereas IP handles the actual delivery of the data, TCP keeps track of the packets that a message is divided into for the efficient routing through the Internet.

Uniform Resource Locator (URL) – Is the address of a resource available on the Internet. Example: the URL for Prince Georges County Fire/EMS is http://www.co.pg.md.us The standard way to give the address of any resource on the Internet that is part of the World Wide Web (www)

Uninterruptible Power Supply (UPS) - A power supply that includes a battery to maintain power in the event of a power outage.

Universal Serial Bus (USB) –, connects devices to computer such as keyboards, mice, PDAs, cameras and printers

Virus – A program that can copy itself and infect computers without permission

VoIP – Voice over Internet Protocol - A category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions of the **P**ublic **S**witched **T**elephone **N**etwork *(*PSTN).

Virtual Private Network (VPN) – A common secure network accessed via the internet. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Web Browser – A software application used to locate and display Web pages. The most popular browsers are Microsoft Internet Explorer and Firefox.

Wide Area Network (WAN) – Wide Area Networks take two or more Local Area Networks (LAN) and link them together, creating a WAN. WANs can be made up of interconnected smaller networks spread throughout a building, state or entire globe.

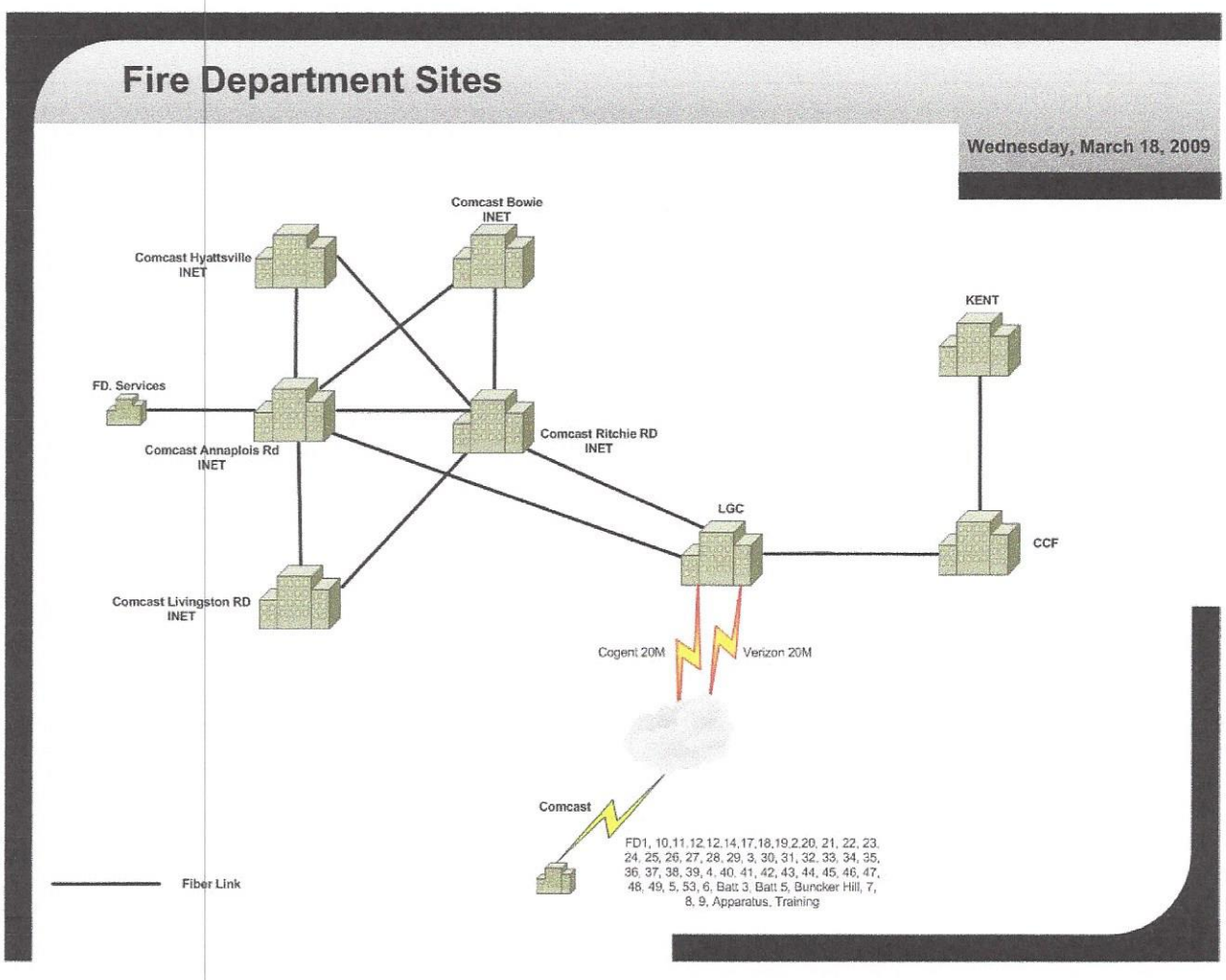
Wireless Access Point – A device that allows wireless communication devices to connect to a network

World Wide Web (WWW) - A system of Internet servers that support specially formatted documents. The documents are formatted in a markup language called HTML (*HyperText Markup Language*) that supports links to other documents, as well as graphics, audio, and video files. This means you can jump from one document to another simply by clicking on hot spots. Not all Internet servers are part of the World Wide Web.

There are several applications called Web browsers that make it easy to access the World Wide Web; Two of the most popular being Netscape Navigator and Microsoft's Internet Explorer.

3.0 The Prince George's County Network

The Office of Information Technology and Communications (OITC) is the centralized support agency responsible for the innovation, implementation and advancement of technologies in Prince Georges County Government. OITC maintains the County's Information Technology Infrastructure which includes both voice and data systems. As such OITC and the Fire/Ems Department have network policies and procedures in place to ensure its security and operability. Following you will find various policies and procedures that will need to be followed in order to maintain a viable working network.



3.1 ELECTRONIC INFORMATION POLICY
ADMINISTRATIVE PROCEDURE 119

SUBJECT: Electronic Information Policy

PURPOSE: Prince George's County Government maintains its computers and the network for users to conduct the business of the County in a timely and efficient manner. The electronic information system and its contents are the property of Prince George's County Government. The phrase "electronic information" refers to electronic and voice mail, Internet access, Intranet access, and the creation of or access to electronic data (whether by word processing, spreadsheet, or other software programs.)

SCOPE: This policy applies to all users of Prince George's County Government Electronic Information Systems, including but not limited to, Prince George's County Government employees, 1000-hour employees, contractors, limited-term grant funded positions and volunteers.

AUTHORITY: Chief Administrative Officer

RESPONSIBILITY: All Prince George's County Government Departments and Agencies

POLICY:
Information and information systems are essential Prince George's County Government assets, each vitally important to Prince George's County Government's business operations and long-term viability. Prince George's County Government must ensure that information and information system assets are protected in a manner that is cost-effective and that reduces the risk of unauthorized information access, disclosure, modification, or destruction, whether accidental or intentional.

The Office of Information Technology and Communications has established the following policy to address the protection, access, and use of Prince George's County Government electronic data and equipment; and, to detail the rights and responsibilities of users of electronic data and equipment.

I. General Use of Electronic Communications Systems

The Office of Information Technology and Communications has established the following Information Technology Policy to provide specific direction on appropriate business use of Prince George's County Government information and telecommunications systems and equipment.

A. *Acceptable Use*

Prince George's County Government information and telecommunications systems and equipment, including computers, laptops, handheld communications devices, Internet, Intranet, electronic mail, telephones, cellular phones, pagers, voice mail, and fax, are provided for official and authorized Prince George's County Government business purposes. Any use of such systems and equipment perceived to be illegal, harassing, offensive, or in violation of other Prince George's County Government policies, standards, or guidelines, or any other uses that would reflect adversely on Prince George's County Government, may be considered a violation of this policy.

B. *Right to Monitor*

Prince George's County Government reserves the right to monitor, record, or periodically audit use of any of its information and telecommunications systems and equipment. Use of these systems and equipment constitutes expressed consent to such monitoring, recording, and auditing. Actual or suspected misuse of these systems should be reported to the appropriate Prince George's County Government management representative in a timely manner.

C. *Privacy and Ownership*

Electronic information created, sent, forwarded, received, or saved on Prince George's County Government electronic information systems is the property of Prince George's County Government and is not considered the private communications of any user. All users are advised that there is no expectation of privacy regarding any information created, sent, received, or stored through or by Prince George's County Government electronic information systems. Such information is the property of Prince George's County Government. Prince George's County Government reserves the right to view and monitor all electronic information created, sent, forwarded, received, or saved on Prince George's County Government electronic information systems without notice. As provided by applicable law, electronic information on Prince George's County Government's systems may be subject to retrieval and disclosure at any time for litigation discovery, Maryland Public Information Act requests, and law enforcement, or other regulatory investigations.

II. Business Conduct Guidelines

A. *Proper Use*

Prince George's County Government electronic information systems are to be used for Prince George's County Government authorized and official business and work-related purposes. Incidental personal use is permissible with the approval of the Appointing Authority as long as the incidental personal use does not interfere with employee productivity; does not preempt any business activity; does not hamper or conflict with the transaction of Prince George's County Government business; and does not consume more than a trivial amount of system resources.

Examples of such use are scheduling medical appointments, communicating with schools, or contacting childcare workers. Such permitted uses are intended to support a family friendly environment, while mitigating the need for the employee's absence from the workplace to conduct such tasks. In all cases, the direct supervisor and, ultimately, the Appointing Authority are responsible for the enforcement of proper use.

Employees are reminded that the use of County government information system resources should never be used inappropriately or create the appearance of inappropriate use.

County electronic communication systems must not be used for:

- Charitable Fundraising
- Religious Advocacy or Religious Activities
- Political Advocacy Efforts or Political Messages
- Private Business Activities
- Personal Amusement And Entertainment
- Soliciting Business or Unauthorized Solicitations Of Any Kind
- Selling Products
- Otherwise Engaging In Commercial Activities
- Transmitting Or Accessing Copyrighted Information In A Way That Violates The Copyright Laws
- Downloading Or Accessing Software Or Data From Another Source That Has Not Been Determined To Be Free Of Viruses
- Personal Gain
- Chain Letters
- Illegal Activities
- Spamming
- Internet Relay Chat (IM through AOL, Yahoo, MSN, etc.)

It is prohibited to use the County's electronic information system to view, create, forward, save, maintain, or send offensive material. Offensive material refers to any inflammatory material; material with abusive language; sexually, culturally, or racially offensive or insulting material; or obscene, vulgar, or profane material.

III. Personally Identifiable Information

The Office of Human Resources Management (OHRM) is the custodian of employee records and the Office of Information Technology Communications (O ITC) is the custodian of employee electronic data. Management and authorized employees must be vigilant in securing the personally identifiable information of employees, customers, citizens, and residents of Prince George's County.

A. Background

As evidenced by recent news reporting stolen electronic personally identifying information, organizations are realizing the devastating effect of public disclosure from inadequate privacy

practices. Extraordinary care must be taken with the use of personally identifiable information; otherwise, we may place this information in the wrong hands.

B. *Definition*

Personally identifiable information is any piece of information that potentially can be used to uniquely identify, contact, or locate an individual. Examples of personally identifiable information include:

1) Full Name;
2) Social Security Number;
3) Telephone Number;
4) Street Address;
5) Email Address;
6) Vehicle Registration Plate Number;
7) Driver's License Number;
8) Face, Fingerprints, or Handwriting,
9) Medical Information,
10) Work Schedules,
11) Picture/Photo Identification,
12) Bank Accounts/Direct Deposit Accounts; and
13) Employment Records.

C. *Points of Information*

Advances in Information Technology have made it easier to collect personally identifiable information resulting in a profitable collection and resale market, as well as criminal exploitation of personally identifiable information through identity theft.

Lawmakers have responded by enacting a series of legislation to limit the distribution and accessibility of personally identifiable information. Several examples of this legislation include:

1) HIPAA, which primarily focuses on protecting personally identifiable health information;

2) the Privacy Act of 2005, recently proposed by the U.S. Senate, which attempts to strictly limit the display, purchase, or sale of personally identifiable information without consent;

3) The Anti-Phishing Act of 2005, which attempts to prevent the acquiring of personally identifiable information through phishing; and

4) The Social Security Number Protection Act of 2005 and Identity Theft Prevention Act of 2005, each seeking to limit the distribution of social security numbers.

D. *Procedure*

Employees in every Prince George's County Government Agency, Department, Division, and organizational unit are immediately requested to observe the following Enterprise Security Guidelines related to access and use of personally identifiable information.

1) Restrict access to personally identifiable information to authorized users. Restrict the ability to create databases, lists, or files that include personal identifying information by those with authorized access to personally identifiable information;

2) Prohibit physical removal of personally identifiable information from Prince George's County Government on removable media (disks, CDs, DVDs, tapes, drives, USB drives) and laptop computers unless expressed written authorization is approved and obtained in advance by the Appointing Authority and forwarded to the Directors of the Office of Human Resources Management and the Office of Information Technology and Communications;

3) Prohibit creation, storage, and posting of databases, lists, or files containing personally identifiable information on local (e.g., C:\ and D:\) drives, network shared (e.g., I:\ or S:\) drives, Internet, Intranet, or electronic mail without the expressed written consent of the Directors of the Office of Human Resources Management and the Office of Information Technology and Communications;

4) Inform employees on the need for securing personally identifiable information. Implement procedures to ensure that personally identifiable information is not improperly created and stored;

5) Conduct an accurate and thorough assessment of any existing databases, lists, and files that contain personally identifiable information;

6) Secure (password protect) or remove any existing databases, lists, and files that contain personally identifiable information from local (e. g., C:\ and D:\) drives, network shared (e.g., I:\ or S:\) drives, Internet, Intranet, and electronic mail;

7) Implement procedures to determine that employee access to personally identifiable information is appropriate;

8) Identify any vulnerability as related to the availability of electronic personally identifiable information. Resolve vulnerabilities or contact the Office of Information Technology and Communications Enterprise Security Manager for assistance;

9) Apply appropriate sanctions against employees who fail to comply with the information presented in this Administrative Procedure, and associated and referenced security policies, standards, guidelines, processes, and procedures. These sanctions may include all applicable federal, state and County laws. Failure to comply with these guidelines may subject employees to severe disciplinary action, up to and including, dismissal and removal as an authorized County user; Any and all users who fail to comply with these guidelines may also be removed as users.

10) Report all incidents of misuse of personally identifiable information to the Office of Information Technology and Communications Enterprise Security Manager;

11) Comply with the Prince Georges County Personnel Law, as may be amended from time to time, which support the County's privacy laws and relate to personally identifiable information:

    a. Personnel Law Section, 16-108 Appointing Authorities, supervisors and employees general responsibilities (include maintaining security of confidential records);

    b. Personnel Law Section, 16-215 Records Policy (confidential information);

    c. Personnel Law Section, 16-217 Departmental or agency personnel files;

    d. Personnel Law Section, 16-238 Use of employee's Social Security account number;

    e. Personnel Procedure #262 Maintenance, Access and Retention of Personnel Files; and

    f. Maryland Public Information Act (MPIA).

The physical removal of any lists, files and/or data from a Department or Agency is prohibited unless expressed written authorization is approved and obtained in advance by the Appointing Authority and forwarded to the Directors of the Office of Human Resources Management and the Office of Information Technology and Communications.

ADDITIONAL POLICIES AND STANDARDS:

The full version of the following Policies and Standards relating to information and information systems: access, disclosure, modification, or destruction is found on the Prince George's County Government Intranet located within the Office of Information Technology and Communications Agency Portal Page. It is the responsibility of all employees to become familiar with and to

comply with all OITC Policies and Standards relating to information and information systems and the associated and referenced guidelines, processes, and procedures.

IV. Electronic Mail Acceptable Use

The Office of Information Technology and Communications has established an Electronic Mail Acceptable Use Standard to provide specific instructions and requirements on the proper and appropriate business use of electronic mail resources.

V. Internet Acceptable Use

The Office of Information Technology and Communications has established an Internet Acceptable Use Standard to provide specific instructions and requirements on the proper and appropriate business use of Internet resources.

VI. Intranet Acceptable Use

The Office of Information Technology and Communications has established an Intranet Acceptable Use Standard to provide specific instructions and requirements on the proper and appropriate business use of Intranet resources.

VII. Electronic Records Retention

The Office of Information Technology and Communications has established an Electronic Records Retention Policy to establish specific requirements and responsibilities for the management and disposition of Prince George's County Government electronic records.

VIII. Access Control

The Office of Information Technology and Communications has established an Access Control Standard to provide specific instructions and requirements for the proper identification, authentication, and authorization controls necessary to access Prince George's County information assets.

IX. Physical Access

The Office of Information Technology and Communications has established a Physical Access Standard to provide specific instructions and requirements for proper controls to physically access Prince George's County Government information assets.

X. Remote Access

The Office of Information Technology and Communications has established a Remote Access Standard to provide specific instructions and requirements for the proper identification, authentication, and authorization controls necessary to remotely access Prince George's County Government information assets.

XI. Security Awareness

The Office of Information Technology and Communications has established a Security Awareness Policy to establish specific standards on the protection of the confidentiality, integrity, and availability of Prince George's County Government information assets.

XII. Hardware Acceptable Use

The Office of Information Technology and Communications has established a Hardware Acceptable Use Standard to provide specific instructions and requirements on the proper and appropriate business use of Prince George's County Government hardware.

XIII. Software Acceptable Use

The Office of Information Technology and Communications has established a Software Acceptable Use Standard to provide specific instructions and requirements on the proper and appropriate business use of Prince George's County Government software.

XIV. Asset Protection

The Office of Information Technology and Communications has established an Asset Protection Policy to establish specific standards on the protection of the confidentiality, integrity, and availability of County Government information assets.

XV. Asset Identification and Classification

The Office of Information Technology and Communications has established an Asset Identification and Classification Policy to establish specific standards on the identification, classification, and labeling of Prince George's County Government information assets.

XVI. Information Classification

The Office of Information Technology and Communications has established an Information Classification Standard to provide specific instructions and requirements for classifying information assets.

ENFORCEMENT:

Appointing Authorities are responsible for implementation and adherence to this Administrative Procedure within their respective Prince George's County Government Departments and Agencies. This Administrative Procedure supersedes all prior policies and any policy drafted by individual Departments and Agencies. All users who violate this Administrative Procedure may be removed, including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Employees may be disciplined for violating this Administrative Procedure in accordance with applicable law.

INFORMATIONAL CONTACT:
Questions about the above Administrative Procedure should be directed to the Office of Information Technology and Communications at (301) 952-5150.

EFFECTIVE DATE:
This Administrative Procedure is effective on date of signature.

03/27/2007
Date

[Original Signed]
Dr. Jacqueline F. Brown
Chief Administrative Officer

PRINCE GEORGE'S COUNTY GOVERNMENT
OFFICE OF INFORMATION TECHNOLOGY AND COMMUNICATIONS

3.2 ELECTRONIC MAIL ACCEPTABLE USE STANDARD

PURPOSE:	As chief architects and administrators of the Prince George's County Government information technology environment, the Office of Information Technology and Communications established the following Information Technology Standard to provide specific instructions and requirements on the proper and appropriate business use of Electronic Mail Resources.
SCOPE:	All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Prince George's County Government premises or who have been granted access to Prince George's County Government information or systems, are covered by this standard and must comply with associated guidelines, and procedures.
AUTHORITY:	Director, Office of Information Technology and Communications
RESPONSIBILITY:	All Prince George's County Agencies, Branches, Departments, and Agency Supported Resources
ORIGINALLY ISSUED:	May 5, 2006
REVISED:	

I. PURPOSE

This *Electronic Mail Acceptable Use Standard* builds on the objectives established in the *Acceptable Use Policy*, and provides specific instructions and requirements on the proper and appropriate business use of Electronic Mail Resources. The Prince George's County *Acceptable Use Policy* defines objectives for establishing specific standards on the appropriate business use of information assets.

II. SCOPE

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Prince George's County Government premises or who have been granted access to Prince George's County Government information or systems, are covered by this policy and must comply with associated standards, guidelines, and procedures.

III. DEFINITIONS

Information Assets are defined in the *Asset Identification and Classification Policy*.

Electronic Mail Resources refer to Prince George's County Government systems, networks, equipment, software, and processes that provide access to and/or use of the electronic mail, including accessing, downloading, transmitting, or storing data and information, as well as the operation of software products and tools.

Objectionable refers to anything that could reasonably be obscene, indecent, harassing, offensive, or any other uses that would reflect adversely on the Prince George's County Government, including but not limited to comments or images that would offend, harass, or threaten someone on the basis of his or her race, color, religion, national origin, gender, sexual preference, or political beliefs.

Users refer to all individuals, groups, or organizations authorized by the Prince George's County Government to access and use Prince George's County Government Electronic Mail Resources.

IV. REQUIREMENTS

A. Business Use

1. Prince George's County Government Electronic Mail Resources are provided primarily for official and authorized Prince George's County Government business use and purposes.

2. Limited personal use of Prince George's County Government Electronic Mail Resources is acceptable as long as it does not interfere with normal business operations, conflict with business interests, or has an adverse impact on the reputation of Prince George's County Government.

3. The use of Prince George's County Government Electronic Mail Resources shall be in accordance with applicable laws and regulations.

4. Users shall be accountable for all Electronic Mail activity associated with their accounts.

5. All electronic mail transmissions outside the Prince George's County Government must have the following disclaimer attached:

> "This E-mail and any of its attachments may contain Prince George's County Government or Prince George's County 7th Circuit Court proprietary information, which is privileged and confidential. This E-mail is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this E-mail, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this E-mail is strictly

prohibited and may be unlawful. If you have received this E-mail in error, please notify the sender immediately and permanently delete the original and any copy of this E-mail and any printout."

B. Improper Use

1. Any use of Prince George's County Government Electronic Mail Resources must not be illegal, must not constitute or be perceived as a conflict of Prince George's County Government interest, must not violate Prince George's County Government policies, and must not interfere with normal business activities and operations.

2. Users shall not violate any laws or regulations using Prince George's County Government Electronic Mail Resources.

3. Prince George's County Government Electronic Mail Resources shall not be used to forward chain letters, virus warnings, and hoaxes or support other such "re-mailing" activities.

4. Prince George's County Government Electronic Mail Resources shall not be used to download, transmit, or store objectionable material, images, or content.

5. Prince George's County Government Electronic Mail Resources shall not be used to conduct personal or non- Prince George's County Government solicitations.

6. Users must not allow others to access Electronic Mail Resources by using their accounts.

C. Electronic Mail Software

1. Only Prince George's County Government approved versions and configurations of electronic mail software may be used. The following electronic mail software is authorized for use:

    - Microsoft Outlook 2000 and Microsoft Outlook 2003

2. Users must not adjust the electronic mail software security settings to be less restrictive than the Prince George's County Government approved configuration.

3. Users shall not use software or features that automatically forward electronic mail messages.

4. Users shall not use software or features (such as an anonymous mail sender) that obscures or masks the identity of the message sender.

D. Downloaded Materials

1. Prince George's County Government Electronic Mail Resources shall not be used to send, receive, or store any commercial software, shareware, or freeware without Prince George's County Government 's prior written authorization.

2. The content and attachments of electronic mail messages must be reviewed for malicious code and viruses in accordance with the *Asset Protection Policy* and the *Anti-Virus Standard*.

3. For security and performance purposes, electronic mail attachments must be less than 10 megabytes.

E. Right to Monitor

1. All Electronic Mail Resources and all messages created, received, processed, transmitted, and/or stored on the Prince George's County Government Electronic Mail Resources are Prince George's County Government information assets and property.

2. Prince George's County Government reserves the right to monitor and review all activities and messages using Prince George's County Government Electronic Mail Resources at any time by authorized Prince George's County Government personnel.

3. Prince George's County Government reserves the right to disclose the nature and content of any user's messages and activities involving Prince George's County Government Electronic Mail Resources to law enforcement officials or other third parties without any prior notice to the user.

F. Privacy Expectations

1. Users should have no expectations of privacy when using Prince George's County Government Electronic Mail Resources.

G. Storage Capacity

1. Users shall delete unnecessary electronic mail message to avoid unnecessary accumulation of storage on the Prince George's County Government electronic mail servers.

2. Electronic mail messages containing business critical information should be stored on production servers to ensure proper data backup.

3. Electronic mail messages are public records when they are created or received in the transaction of public business. They must be retained as evidence of official policies, actions, decisions or transactions. E-mail messages are considered public record material with legally mandated retention requirements, and are subject to the same rules and regulations as those governing the management of paper records. Electronic mail is managed by its content, not its format.

H. Misuse Reporting

1. Actual or suspected misuse of Prince George's County Government Electronic Mail Resources should be reported in accordance with the *Misuse Reporting Standard*.

2. Upon the receipt or continued receipt of objectionable electronic mail, users should contact their immediate supervisor in accordance with the *Misuse Reporting Standard*.

V. RESPONSIBILITIES

The Director of the Office of Information Technology and Communications is the approval authority for the *Electronic Mail Acceptable Use Standard.*

The Director of the Office of Information Technology and Communications in conjunction with the Enterprise Security Manager is responsible for the development, implementation, and maintenance of the *Electronic Mail Acceptable Use Standard* and associated guidelines and procedures.

Prince George's County Government management is responsible for ensuring that the *Electronic Mail Acceptable Use Standard* is properly communicated and understood within its respective organizational units. Prince George's County Government management also is responsible for defining, approving, and implementing processes and procedures in its organizational units, and ensuring their consistency with the *Electronic Mail Acceptable Use Standard.*

Users are responsible for familiarizing themselves and complying with the *Electronic Mail Acceptable Use Standard* and the associated guidelines provided by Prince George's County Government management. Users also are responsible for reporting misuse of Prince George's County Government Electronic Mail Resources to management, and cooperating with official Prince George's County Government security investigations relating to misuse of such resources.

VI. ENFORCEMENT AND EXCEPTION HANDLING

Failure to comply with the *Electronic Mail Acceptable Use Standard* and associated guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Request for exceptions to the *Electronic Mail Acceptable Use Standard* should be made by submitting the *Information Technology Exception Request Form* to the Director of the Office of Information Technology and Communications, 9201 Basil Court, Suite 270, Largo, MD 20774, or email oitcdirector@co.pg.md.us. Prior to official management approval of any exception request, the individuals, groups, or organizations identified in the scope of this process will continue to observe the *Electronic Mail Acceptable Use Standard.*

VII. REVIEW AND REVISION

The *Electronic Mail Acceptable Use Standard* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: [Original Signed] Date: _____
Charles W. Wilson
Director, Office of Information Technology and Communications

3.3 Prince George's County Fire/EMS Department Confidentiality Agreement

PURPOSE

Confidentiality measures are taken to assure that all Prince George's County Fire/EMS Department employees, agents, vendors or contractors, hold information used or obtained in the course of their duties in confidence. The responsibility for maintaining confidentiality of information lies with the individual entrusted with the information. Implicit in the trust is the expectation that the individual will not divulge information, nor gain access to information, unless there is necessity based on the job description or standards of practice.

POLICY

Access to computer systems and proprietary information is determined by the job responsibilities of the individual seeking access and is to be controlled and monitored through management oversight and identification authentication practices. Access to computer information systems is to be controlled, at a minimum, by the use of individualized and confidential user sign-on/password codes.

Prince George's County Fire/EMS Department employees, contractors, vendors, and other agents of Prince George's County who will have access to confidential information through normal job functions will be issued confidential and individualized sign-on codes. Before a sign-on code is issued, a user must sign a *Computer User Confidentiality Agreement*, which acknowledges their commitment to protect and maintain the confidentiality of the following:

- their sign-on code(s) and password(s),
- all patient and or Fire/EMS Department personnel information
- all proprietary information to which they have access in the course of their work.

When users sign the *Computer User Confidentiality Agreement* they attest that they read and understand the consequences of violating the agreement.

CONSEQUENCES OF VIOLATION OF CONFIDENTIALITY

The consequences of violating the confidentiality of data, a user sign-on code, or other Prince George's County Fire/EMS Department or County proprietary data, may result in immediate suspension of access privileges, as well as disciplinary action, up to and including termination. Violation of confidentiality may also create civil and criminal liability.

MONITORING ACCESS TO CONFIDENTIAL DATA

Information Management and the County's Office of Information Technology & Communications (OITC) will monitor use of the systems and will report access or confidentiality violations immediately to the appropriate OITC Liaison and to the Agency Director. All staff and employees are responsible for immediately reporting any apparent violations of this confidentiality policy to their Managers for action.

Prince George's County Fire/EMS Department
Computer User Confidentiality Agreement

I, the undersigned, acknowledge that in the course of my work at the Prince George's County Fire/EMS Department I will be privileged to information confidential to Prince George's County, the Prince George's County Fire/EMS Department, or to an individual or employee. I acknowledge receipt of my sign-on code to the County network and systems and understand the following:

1) The sign-on and password code(s) that allow me access to County systems are equivalent to my signature and I will not share the passwords with anyone.
2) I will be responsible for any use or misuse of my network or application system sign-on code(s).
3) If I have reason to believe that the confidentiality of my password has been compromised, I will change my password. I will immediately report any known or suspected breach of the confidentiality of the system or records/data obtained from it to my immediate supervisor or the Information Management.
4) It is my responsibility to log out of the system. I will not, under any circumstances, leave unattended a computer terminal to which I have logged on.
5) I will use confidential information only as needed by me to perform my legitimate duties as a Prince George's County Fire/EMS Department employee, contract personnel, vendor, or other agent of Prince George's County. This means, among other things, that:
   a) I will not access confidential information that I have no legitimate need to know.
   b) I will not in any way divulge, copy, release, sell, loan, revise, alter, or destroy any confidential information, except as properly authorized within the scope of my employment.
   c) I will not misuse, or carelessly care for, or fail to safeguard, confidential information.
6) I understand that Information Management and the County's Office of Information Technology & Communications (OITC) conducts and maintains an audit trail of accesses to all information that records the machine name, user, date, and that data is electronically maintained.
7) I have read and agree to all of the above as conditions of being granted a User ID and Password.
8) This agreement will be on file in Information Management. I may review the agreement by contacting the Information Management Manager.

I, the undersigned, further understand and agree that the consequences of a violation of the above statements may result in disciplinary action up to and including termination of employment or contract and or civil/criminal action.

<table>
<tr><td colspan="2">Last Name (Printed)</td><td colspan="2">First Name (Printed)</td><td>Middle Initial</td></tr>
<tr><td colspan="3">Employee Signature</td><td colspan="2">Date</td></tr>
<tr><td colspan="3">Employee Division/Station</td><td colspan="2">Employee Telephone</td></tr>
<tr><td colspan="3">Information Management Approval:</td><td colspan="2"></td></tr>
<tr><td colspan="3">IM Manager Signature</td><td colspan="2">Date</td></tr>
<tr><td>Logon ID Assigned</td><td>User Security Group</td><td>Date</td><td colspan="2">Assigned By</td></tr>
</table>

3.4 Prince George's County Fire/EMS Department Account Request Form

All requests for access must be accompanied by a completed Computer User Confidentiality Agreement.

User Information ***Please print or type all information. All fields must be completed; incomplete forms will be returned***		
Last Name	First Name	Middle Initial
Employee Title		Employee Telephone
HIPPA Training Completed? Yes☐ No ☐	Employee Work Location – Building/Station	
Employee Work Location – Address		Employee Work Location - Room Number

User Signature ***By signing below I indicate that I have read, understand, and signed a Computer User Confidentiality Agreement.***	
Employee Signature	Date

Access Type ***Do not use this form to request access to MILES, NCIC or the District Court systems. Access to these systems is requested using State forms.***	
☐ Network Logon (PGCNT)	☐ Zoll Data Systems Fire Records Management (RMS)
☐ E-mail Account (Outlook)	☐ PDSI Telestaff ☐ County Mainframe

Approval ***All requests for access must be approved at the Battalion Chie, Division Manager, Volunteer Chief, Volunteer President level or above***	
Signature	Date

- - - - - - - - - - Information Management Use Only - - - - - - - - - -				
Date Received	Date Submitted	Magic Ticket Number	Date Returned	Operator
Logon ID Assigned	User Security Group		Date	

3.5 Logon Procedures

What are Logon Procedures

A logon grants user access to a computer or a computer network. It enables personnel to share resources that are on the network. A logon procedure securely verifies who is entering the computer or network/application based on a combination of a user's identification and password.

Logon Procedures

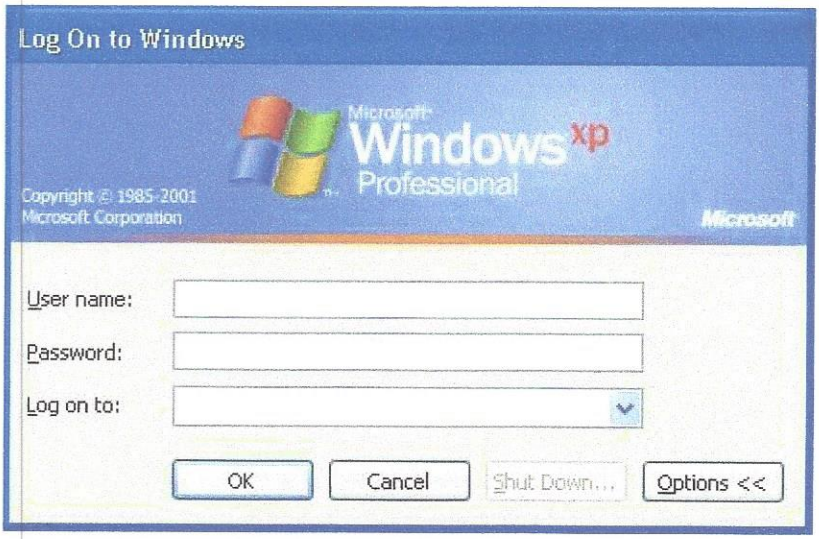
The following set of instructions explains how to logon and access the County's and Department's computer network and applications that are frequently used. The current network logon policy as written by OITC (Office of Information Technology and Communications) requires all County personnel to change their network password every 90 days. A network password should never get used twice and must consist of at least eight (8) characters in length including at least one (1) uppercase letter and at least one (1) number.

All users' names for Network access, Citrix and RMS uses your first initial, middle initial, and last name, for example; Steven J Cooley's username would be SJCooley. The user name for Telestaff is your Fire/EMS Department ID number. The default password for Telestaff is 1234.

3.5.1 Logging onto the County Computer

All Fire/EMS and civilian personnel have logon rights to into the Counties Network. Logging into the Network requires each user to have a user name and password. Your username consist of your first initial, middle initial and your last name, example if your name was Steven J.Cooley, your username would be SJCooley. Default passwords are set by IMD and will allow the users to reset the password back to your personal password. From the image below, the user provides the following to fill in the Windows Login screen;

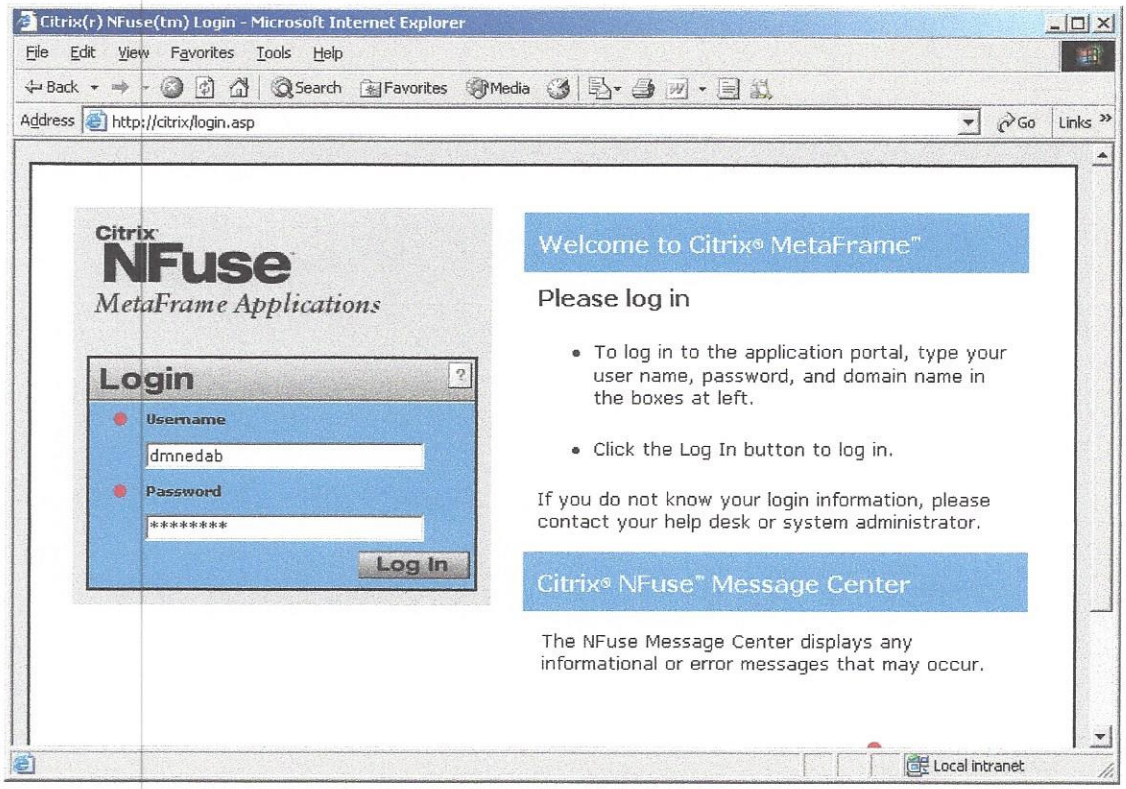
- Username = SJCooley
- Password = user defined (at least eight (8) characters including an upper case letter and a number)
- Log on to = PGCNT (domain)



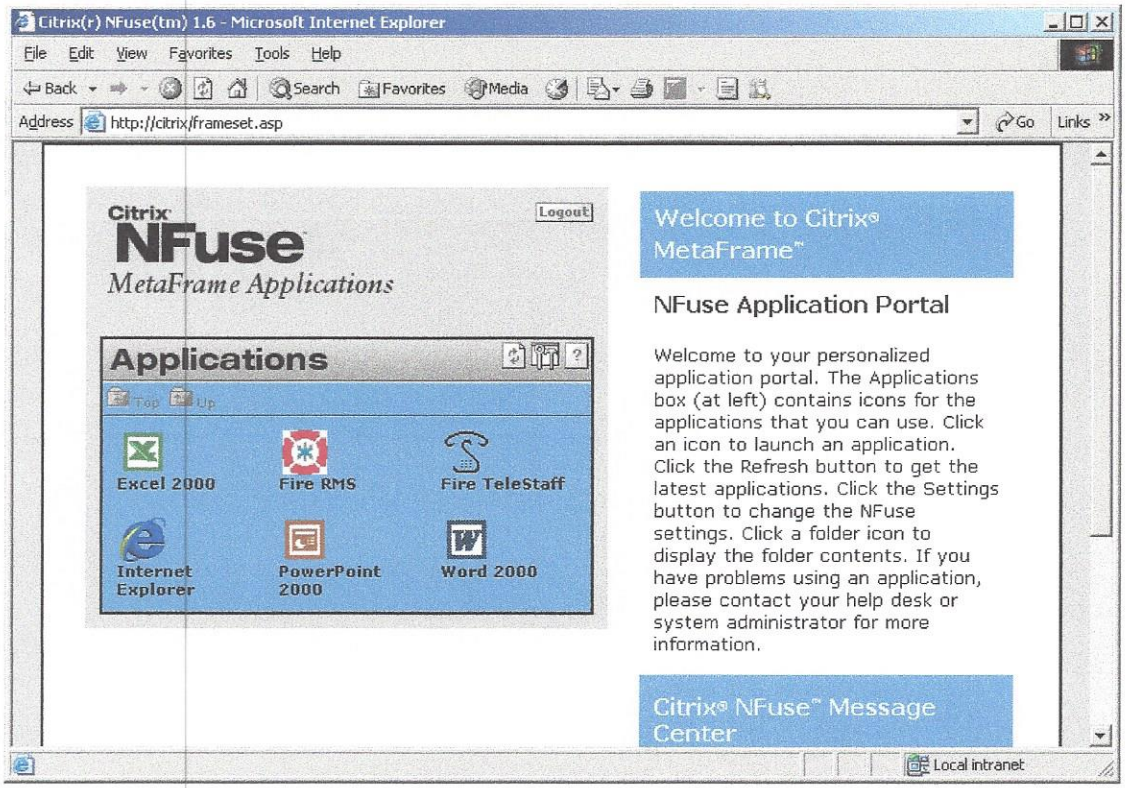
3.5.2 Logging onto Citrix

1. From your web browser type http://citrix/login.asp

2. Logging into Citrix for the first (1st) requires the users to down load the Citrix Client software. Double click on the Citrix ICA Web for 32 –bit Windows located at the bottom right of the Citrix login screen. 1) Double click on the "OPEN" the installation begins. 2) Click on "yes" to allow the installation. 3) Click "yes" to agree to the license agreement information. Upon completion close out of your Web browser and log back into Citrix.



Log in using your Network/Microsoft Outlook username and password. You now have access to the programs listed under the applications window. Double click on the desired software application icon.

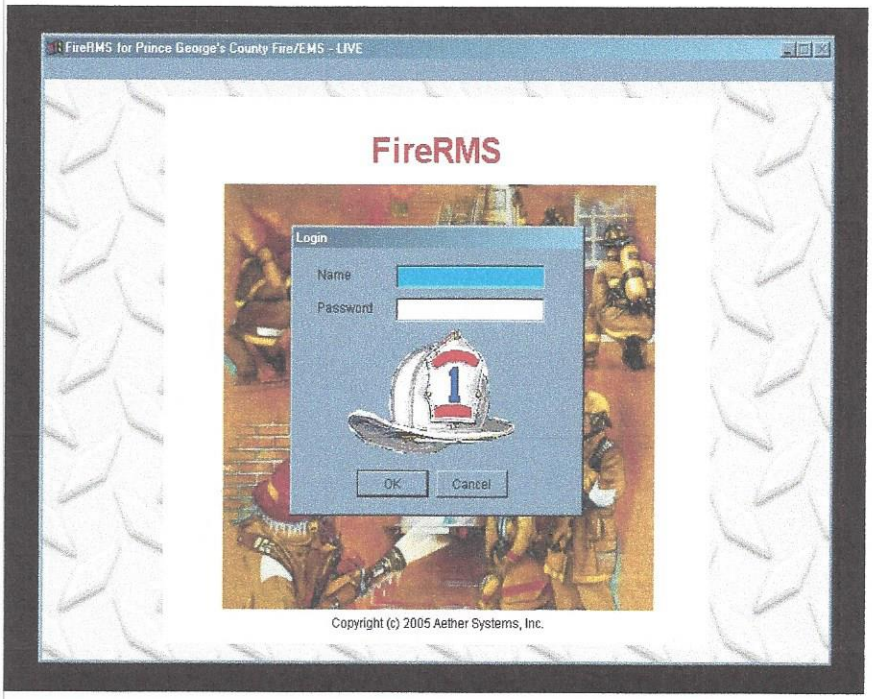


3.5.3 Logging on to RMS

From Citrix, through your web browser, double click the RMS icon.

Firerms.lnk

- Enter name – first and middle initial and last name.
- If no middle name – first initial and last name.
- Enter password (contact Information Management if you need an RMS password)
- Click "OK" button

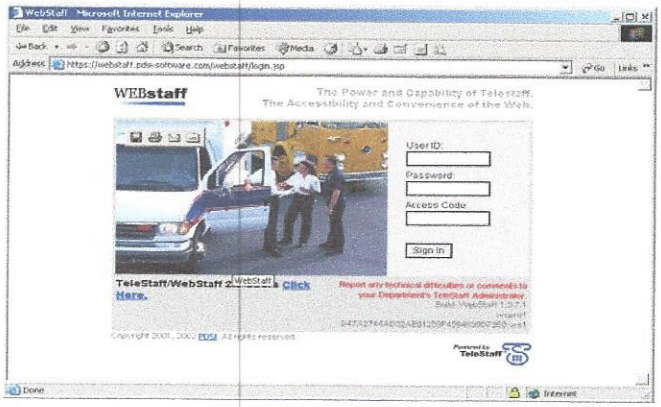


3.5.4 Logging on to Telestaff

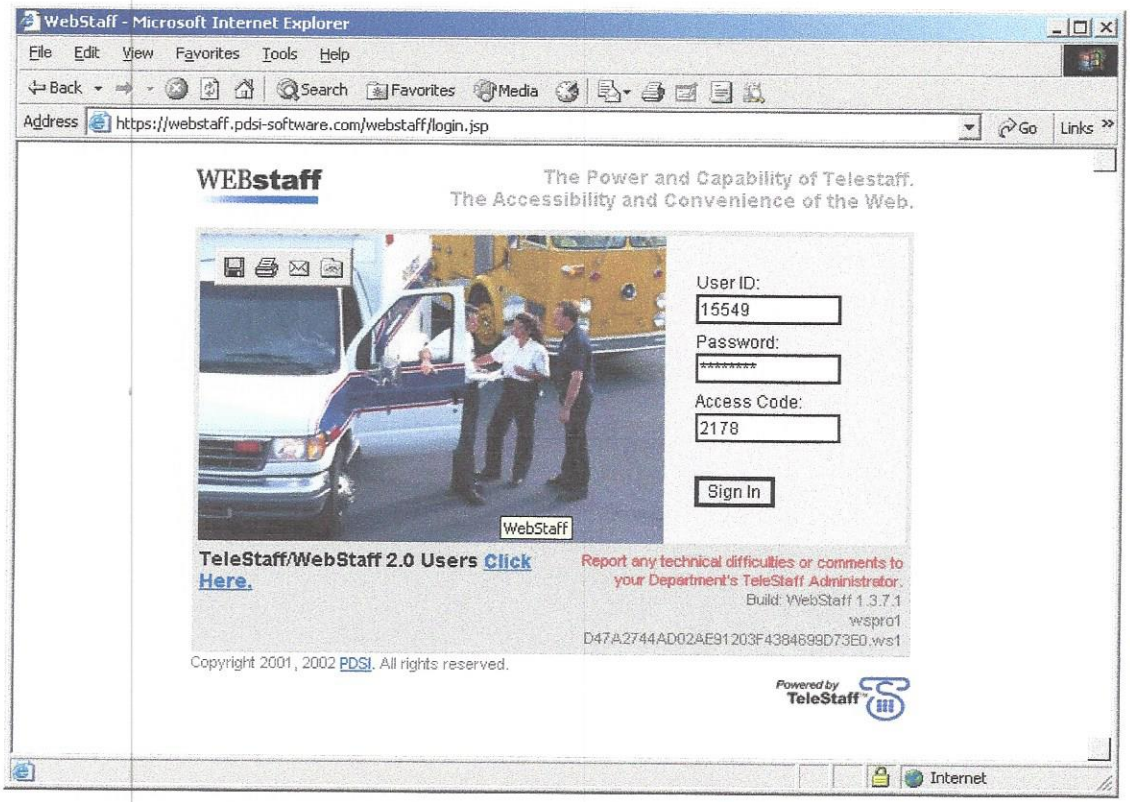
From Citrix through your web browser, double click the Telestaff icon.

- Enter your employee number in the ID prompt.
- If this is your first time logging on Enter 1234 as your password.
- Click 'OK'.

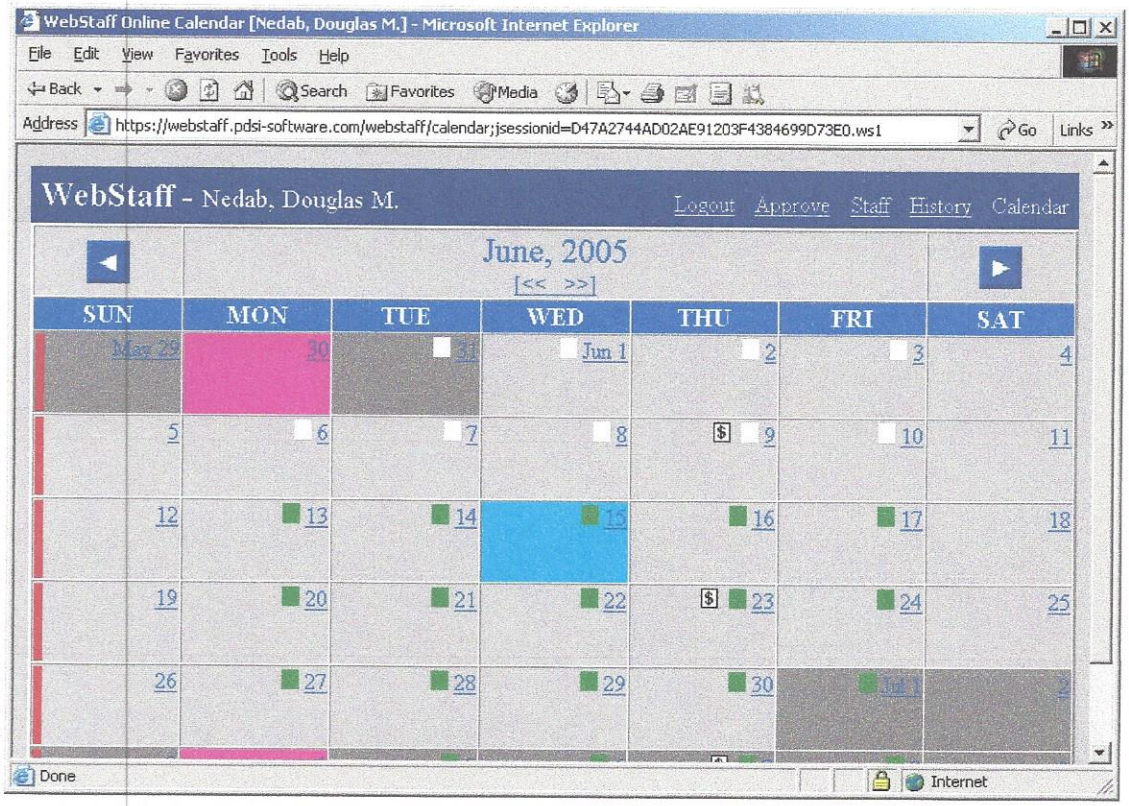
3.5.5 Logging onto TeleStaff via the Internet (WebStaff)



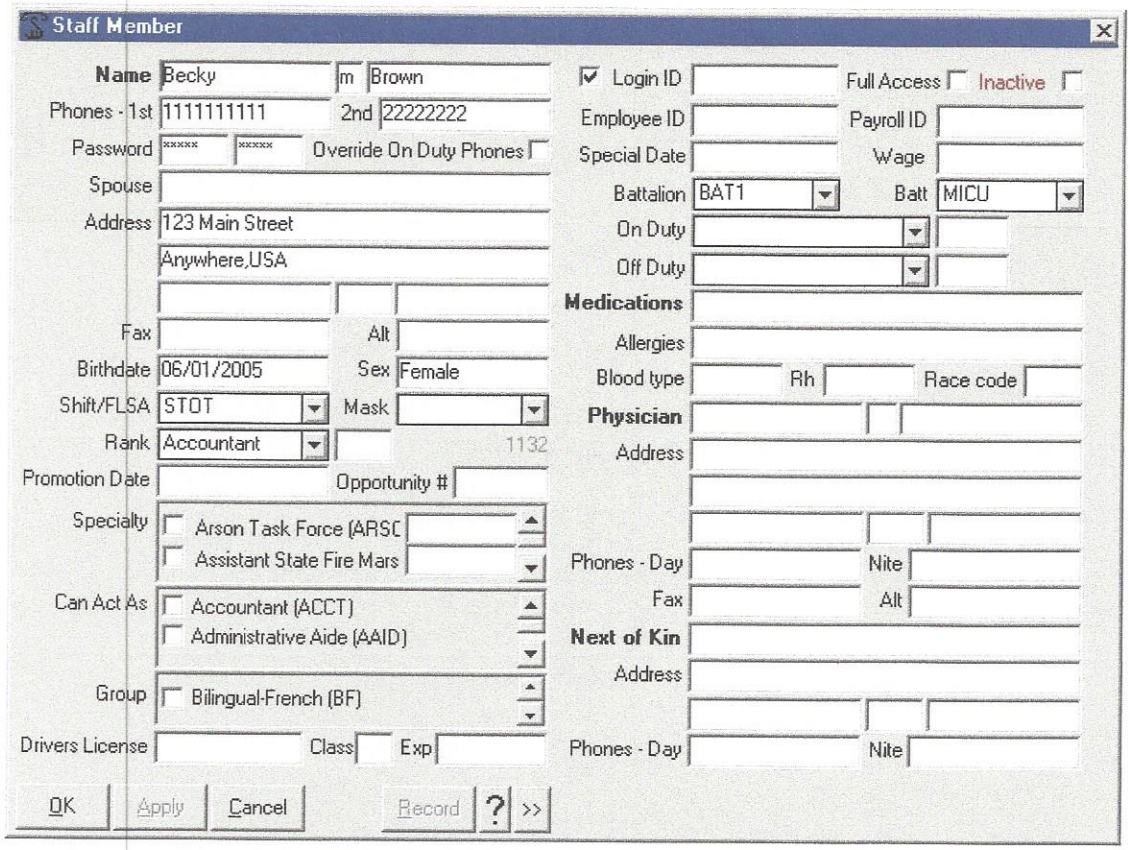
1. Using any web browser go to the TeleStaff website located at https://webstaff.pdsi-software.com/webstaff-2.0/



2. Enter your Fire Department ID # (5 digits), enter your password (1234) first time login and your County access code (2178)



3. You are now logged into Telestaff via the internet. You can make yourself available for overtime or unapproved leave. Contact your Manager or Officer informing them that your calendar is updated and waiting for approval.



You can also update your personal information by double clicking on the Staff icon located at the tip of the page.

3.5.6 Logging on to Microsoft Outlook

1. Double click the Microsoft Outlook Icon on you desktop

Microsoft Outlook.lnk

2. Once the correct profile is chosen from the drop down menu, a box will appear with the following information:

   User Name

   Domain Name PGCNT

   Password

3. Type in the User Name given to you by Information Management
4. Tab down to the Domain Name box. The Domain Name is **pgcnt**
5. Tab down to the Password box to type in the password.
6. Press the enter key or the OK button. This will open your "Inbox"
7. To log out of Microsoft Outlook (the quickest method), click the 'X" located in the upper right hand corner of the screen. A window will appear that reads " Please wait while Microsoft Outlook exits. " You will then be back to your desktop.

3.6 Outlook Profile Setup Instructions

1. From your desktop click start and trace up to Settings over to Control Panel and double click the Mail icon


Mail.lnk

2. A "Properties" Box will appear. Click on the "Show Profiles" button.
3. At the next window click "Add Profiles" button. **(If you need to remove a profile: Select the name to be removed and click "Remove" and then click "Yes").**
4. The "Inbox Setup Wizard" will appear
5. Click "Manually configure information services"
6. Click next
7. In the Profile name box type in the user name (First Name, Middle Initial, and Last name)
8. Click next
9. At the next screen click "Add". The "Add Service to Profile" box will appear
10. Highlight "Microsoft Exchange Server, then click OK.
11. In the Microsoft Exchange server field type "PGEXCHIS01". In the "Mailbox" field type the user's last name; Click the "Check Name" box.
12. NT will ask you to log in. Enter the User's Name, Domain, and Password. **(domain name is pgcnt)**
13. If a list of names is returned, highlight the correct one and click OK.
14. The system will look for the name and will come back with the user's full display name underlined.
15. Click on the "Advanced" tab, and select "None' for "Logon Network Security".
16. Click OK
17. From the "Properties" Screen, Select ADD
18. Select "Outlook Address Book"
19. Click "OK". *Note* - do not select the Personal Address book. The Personal Address book will only work from the user's primary workstation. The Outlook Address Book maintains address information on the Outlook server and will be available wherever you log in.

Test the Setup by logging onto "Outlook" from the Workstation.

3.7 VPN Client Installation Instructions

3.7.1 Installing VPN on your home PC (only)

These instructions provide guidance for installing VPN, McAfee V7.1, and DynaComm on your home PC used to access the County's network and mainframe systems. Perform these instructions in the order as shown (i.e., A, B, C, etc…), unless the instructions dictate otherwise or a particular installation is not needed (e.g., users who do not access Mainframe applications may elect not to install DynaComm)

DOWNLOAD Ciscovpn client_xp_2000_Vista CLIENT

1. Right click on start and select explore, then type in ftp://ftp.co.pg.md.us/
2. Press **ENTER**.
3. Type **public** as the Username and **h0llyw00d** (0=Zero) as the password from the *Login in* pop-up screen.
4. Click **logon**.
5. Right-click on the **Ciscovpn client_xp_2000_Vista CLIENT** Folder.
6. Click **Copy** paste to your C: drive
7. Once Download is completed Click **Close**.

B) PERFORM THESE STEPS TO INSTALL MCAFEE V7.1 (IF NEEDED)

Note: If you already have up to date Virus Protection Software or McAfee 7.1 installed on your computer, PROCEED TO SECTION C.

1. Double-click the **V7.1.EXE** icon.
2. Click **Save** on the *File Download* dialog box.
3. Select **a preferred folder location or folder titled "OITC Downloads"** from the *Save in* drop-down list box on the Save As window.
4. Select **Save** to save the file to your preferred folder or "OITC Downloads".
5. Once Download is completed Click **Close**.
6. Double-click the **V7.1.EXE** icon from your desktop to begin the installation.
7. Click **OK (Winzip.self extractor)**.
8. Click **Setup** to install McAfee Virus Software.
9. Upon successful completion of the install, Click **OK**

Go back to your Internet Browser still showing ftp://ftp.co.pg.md.us

C) PERFORM THESE STEPS TO INSTALL DYNACOMM (*IF ACCESS TO THE MAINFRAME IS NEEDED*)

1. Double-click the **Dynacomm.EXE** icon.
2. Click **Save** on the *File Download* dialog box.

3. Select **a preferred folder location or folder titled "OITC Downloads"** from the *Save in* drop-down list box on the Save As window.
4. Select **Save** to save the file to your preferred folder or "OITC Downloads".
5. Once Download is completed Click **Close**.
6. Double-click the **DYNACOMM.EXE** icon from your desktop to begin installation.
7. Once the installation is completed it will put an icon (lgc mainframe) on your desktop.

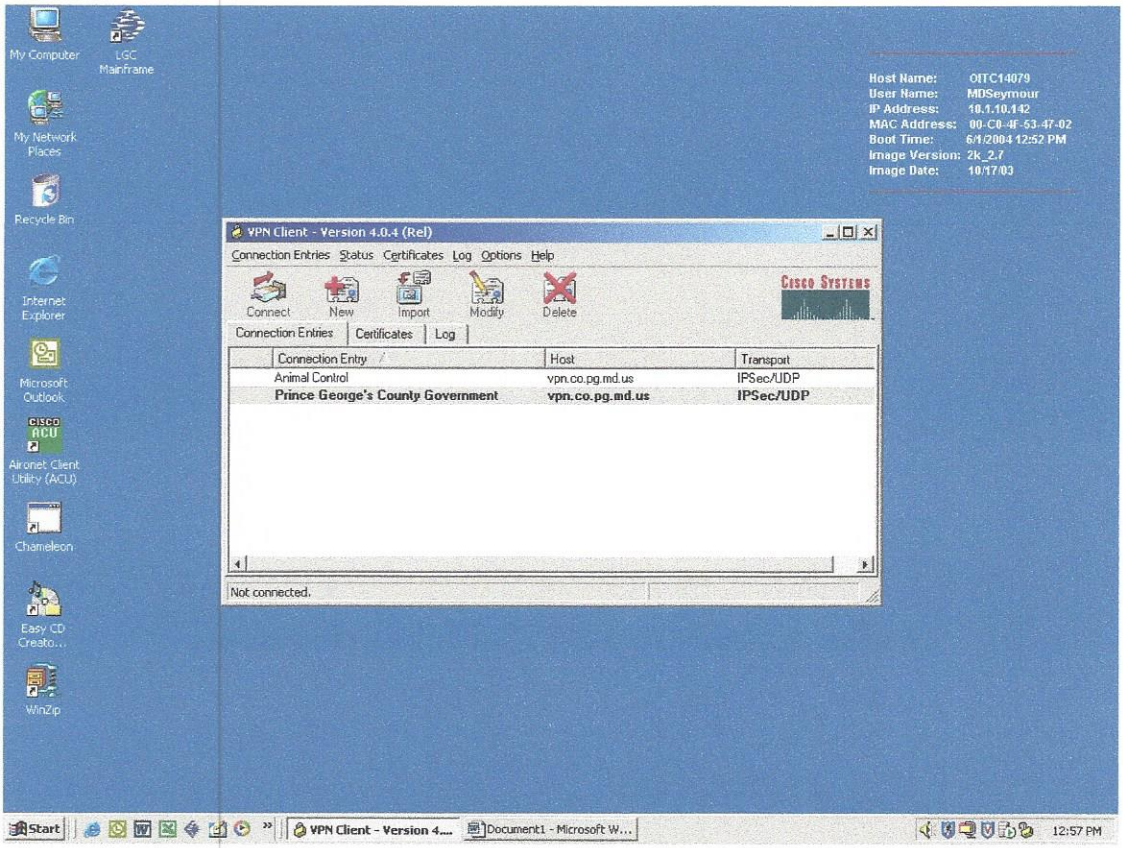
Go back to your Internet Browser still showing ftp://ftp.co.pg.md.us

D) PERFORM THE FOLLOWING STEPS TO INSTALL Ciscovpn client_xp_2000_Vista CLIENT

1. Double click on the folder to install the client

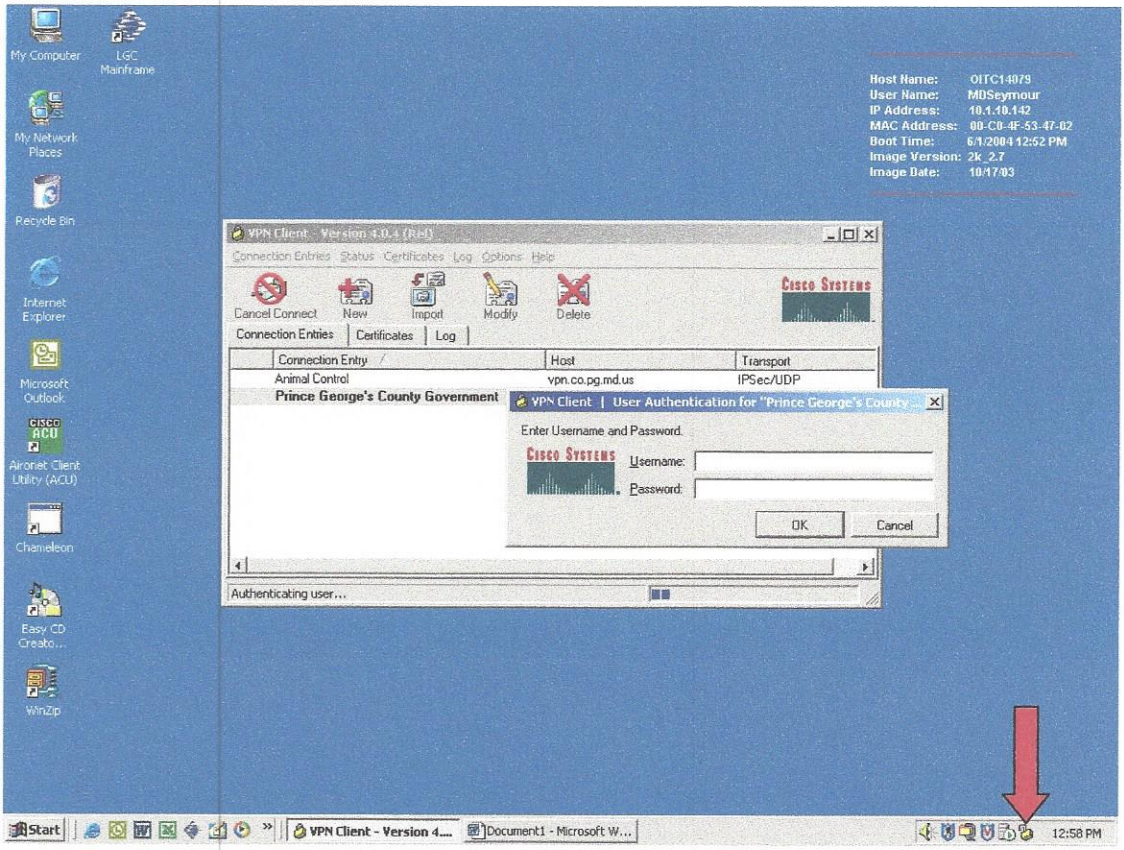
E) VPN CONNECTION

1) Click **Start**.
2) Go to **Programs**.
3) Go to **Cisco VPN Client**.
4) Click **VPN Client** to open the VPN Client window.
5) Click **New** at the top.
6) Go to the **Connection Entry** box and type in **Prince George's County Government**.
7) Go to the **Host** box and type in **vpn.co.pg.md.us**.
8) Go to the **Name** box under **Group Authentication** and type in your **group name** - ***pgcvpn***
9) Go to the **Password** box and type **vpn20774**
10) Go to the **confirm password** box and type **vpn20774**
11) Click **Save**.
12) Click **Connect**.



VPN CONNECTION (Continued)

13) When prompted, enter your **Domain username** and **password**. (*The Domain Username and password is the same as your network logon.*)



14) Click **OK**.

Note: The system tray at the bottom right corner on your screen will display a yellow lock in the locked position—indicating that you are successfully connected to the Prince Georges County network.

15) When the VPN | Client Banner pops up, read it and Click **Continue**.

16) You are now able to perform your usual work routine.

17) To disconnect, Right-click the yellow lock in the system tray and select **Disconnect**.

To access your network drives do the following:

1) Click Start.
2) Click Run.
3) Type the following: \\pgcdc1
4) Click OK.
5) Double click on netlogon.
6) Find .bat **(Please search to find your agency bat file name)**
7) Click on the bat file.
8) Right click and select copy.
7) Right click and select Paste to Copy the bat file to your desktop.

3.7.2 VPN Instructions for MacIntosh (Mac)

Go to ftp.co.pg.md.us

Username – public
Password – h0llyw00d 0=zero

Download the MAC-vpnclient-drawin

Once install please configure the client:

Connection entry - Prince Georges County
Hostname – vpn.co.pg.md.us

Group authentication – pgcvpn
Password – vpn20774

3.7.3 VPN ACCESS VIA THE INTERNET

Please use http://webvpn.co.pg.md.us for VPN access.

Active X will install. Please select the default setting.

After you connected via VPN do the following to access your network drives if needed:

1) Click Start.

2) Click Run.

3) Type the following: \\pgcdc1

4) Click OK.

5) Double click on netlogon.

6) Find firevfr.bat

7) Click on the bat file.

8) Right click and select copy.

9) Right click and select Paste to Copy the bat file to your desktop.

10) Double click on the bat file that you paste to your desktop to run the program.

It will ask for your username and password - (username-pgcnt\xxxxxx) xxxxx=username

3.8 Wireless Routers

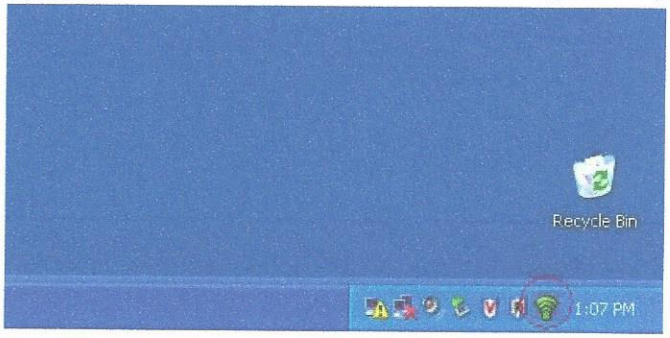
A wireless router has been installed in the majority of the fire stations and administrative offices. Following are instructions on how to access the Prince Georges County's wireless network. Note that there are two sets of instructions – one set for persons who do not have a County network logon and one set of instructions for those persons who do have a County network logon. All persons who would like to access the internet via the wireless router must follow these instructions. For those who have been assigned a County laptop, you may need to bring the laptop to Information Management so that additional software can be installed and for additional instructions. If there are any problems or questions, please contact Information Management via email at **PGFDInformationManagemement@co.pg.md.us** or by calling 301-883-7183.

3.8.1 County User Access Instructions

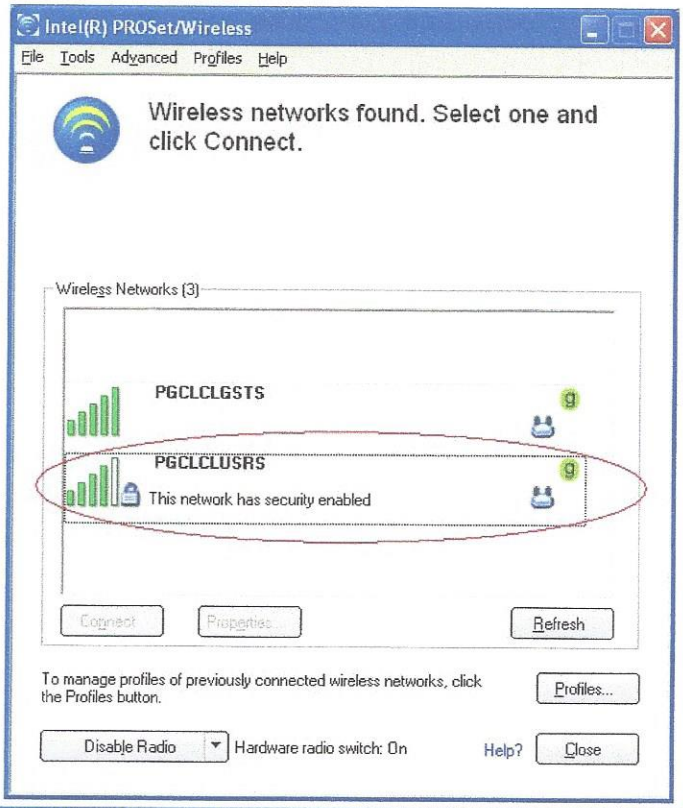
These instructions provide guidance for configuring your wireless Network Interface Card to access the Prince George's County wireless network. NOTE: A service request for Wireless Access may need to be submitted to Information Management (301-883-7183) or via email PGFDInformationManagement@co.pg.md.us before you can access the County's wireless network.

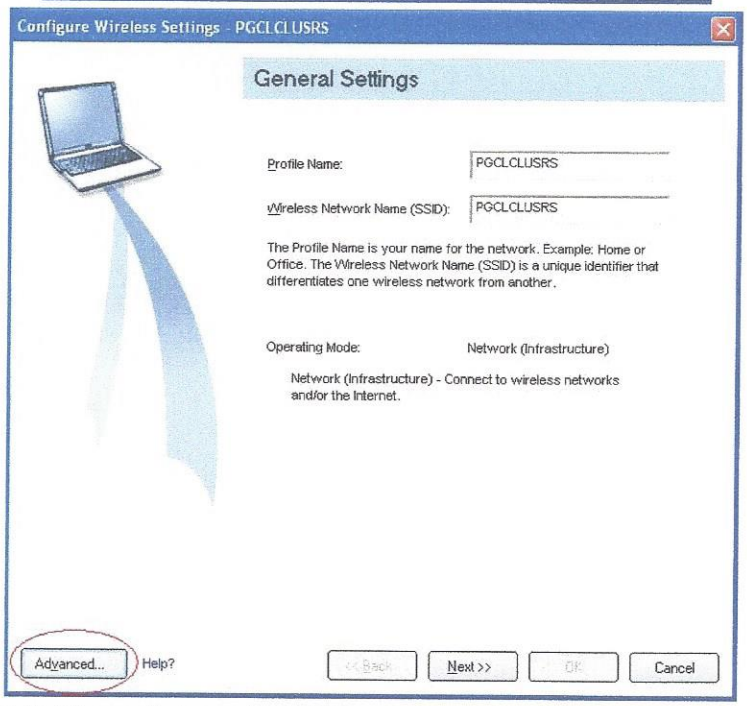
THE FOLLOWING STEPS ARE PERFORMED ON YOUR COUNTY LAPTOP:

8. Double Click on the **Intel PROSet/Wireless Utility** in the system tray.

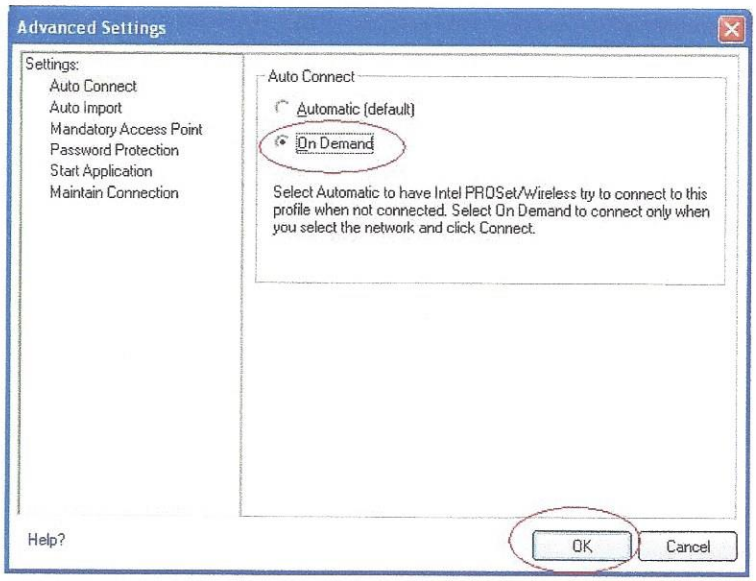


9. The next window will show the **Wireless Networks found** in the area.
10. Look for the SSID **PGCLCLUSRS** or **PGCRMTUSRS** and double click on it.

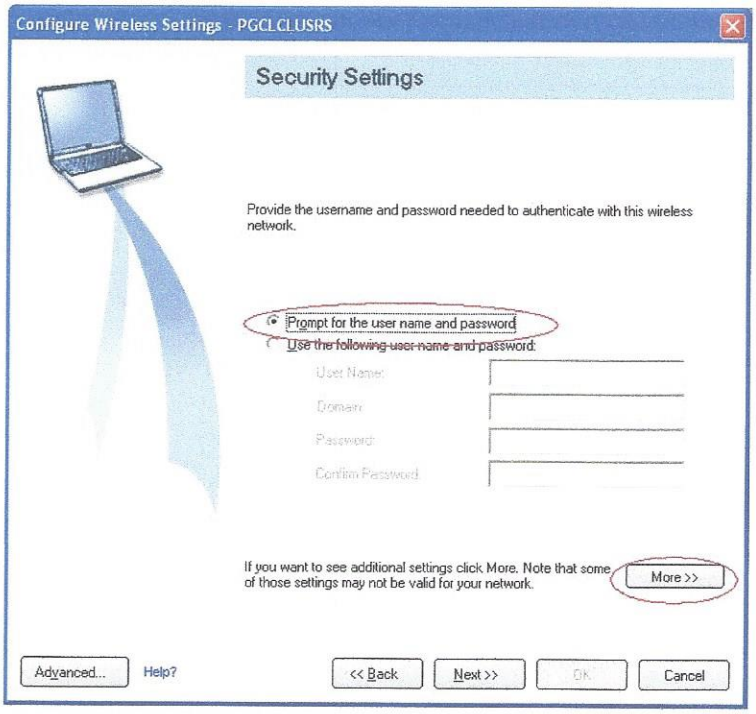




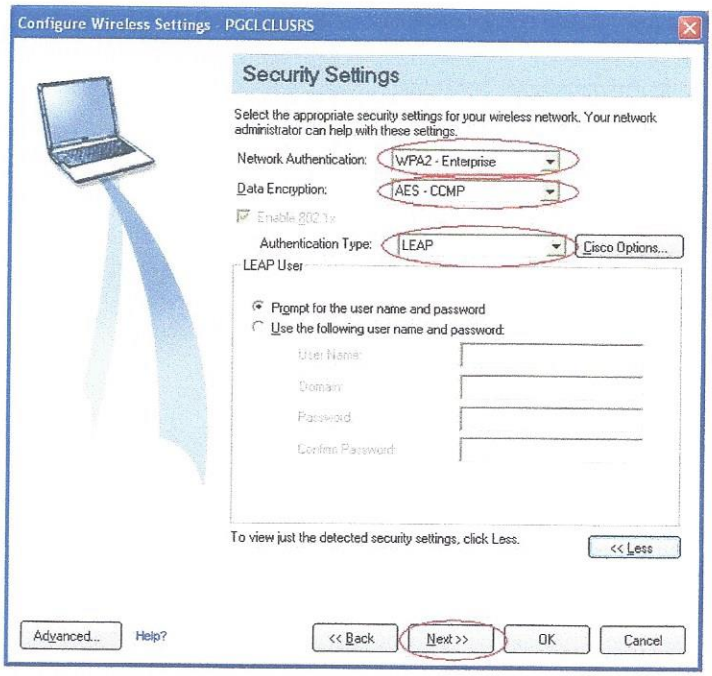
11. On the **General Settings** windows, the SSID you chose should be in the **Profile Name** and **Wireless Network Name(SSID)**.
12. You may change the **Profile Name**, *ie: Work or County Wireless* (optional).
13. Click **Advanced.**



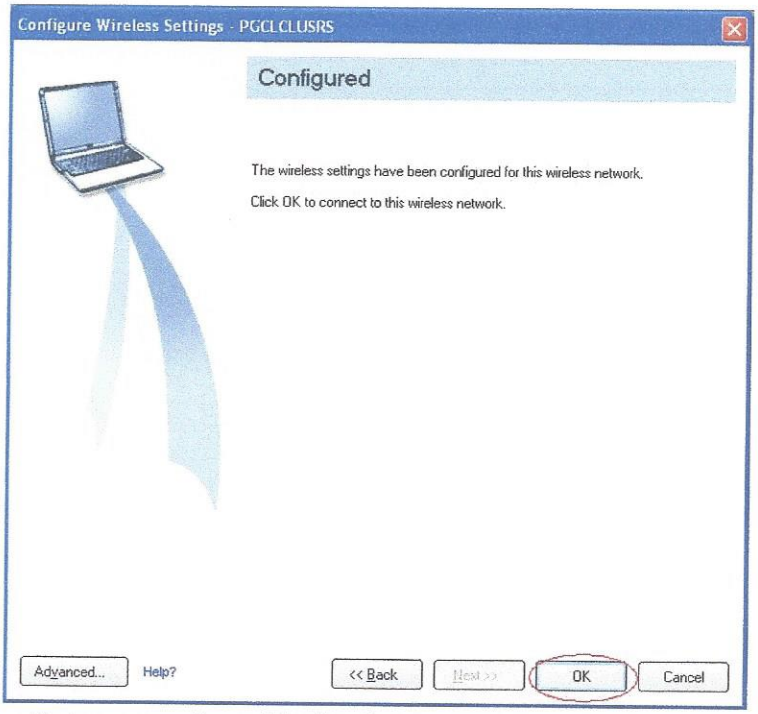
14. In the **Advanced Settings** window set **Auto Connect** to **On Demand**
15. Click **OK** to get back to the previous window, then click **Next.**



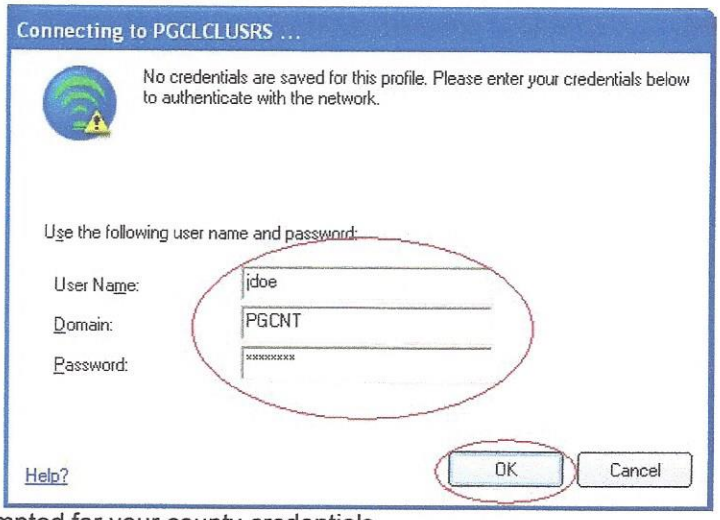
16. On the **Security Settings** window, select **Prompt for the user name and password** then click **More**.



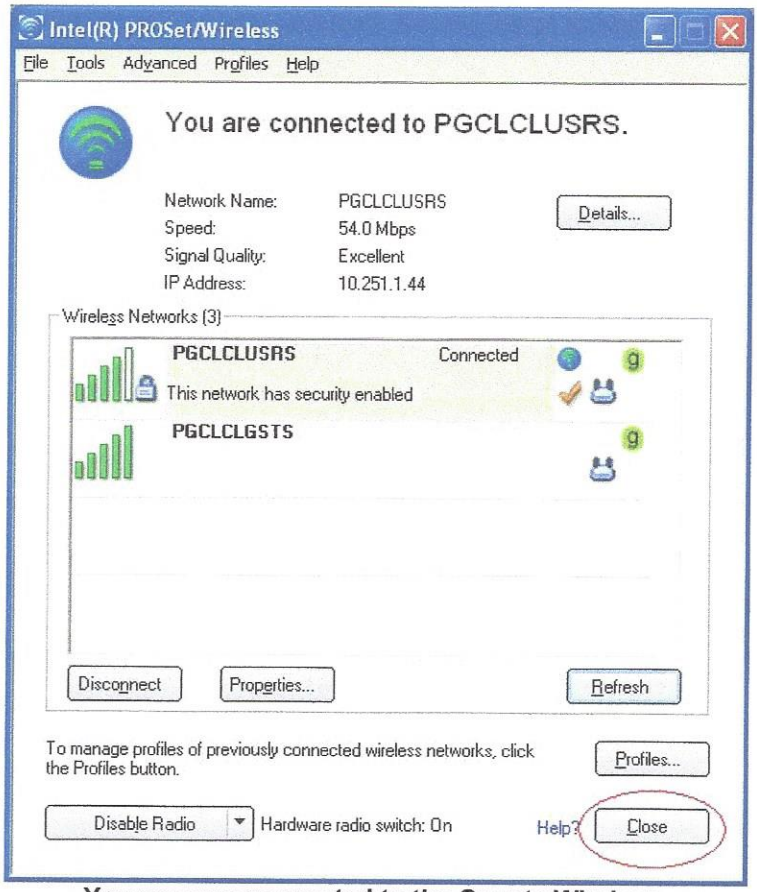
17. Next, on the **Network Authentication** drop box select: **WPA2 - Enterprise**.
18. On the **Data Encryption** drop box select: **AES - CCMP**.
19. On the **Authentication Type** drop box select: **LEAP.**
20. Click **Next.**



21. The wireless profile is now configured for the County Wireless, click **OK.**



22. You will be prompted for your county credentials.
23. Enter you county **Username.**
24. For **Domain**, enter **PGCNT.**
25. Enter your county **Password.**
26. Click **OK.**



You are now connected to the County Wireless.
You can close the Intel PROSet/Wireless Utility.

NOTE: To connect to the County Wireless in the future, you will only need to complete Steps 1 and 2 of the document.

3.8.2 Request for Guest Wireless Account

Information Management can generate wireless access/user accounts to Departmental staff via the wireless routers throughout its administrative offices and the Fire Stations. If you are using your personal laptop or a non county supplied computer to connect to the Internet, a temporary GUEST account must be created for your use.

If County employees require wireless access, please email Information Management at PGFDInformationManagement@co.pg.md.us. The conformation and password to access the Internet will be sent to your County email. This password expires every 14 days and the request must be submitted after each expiration period.

3.9 Checking Network Problems

The purpose of this section is to establish guidelines for reporting problems with Personal Computer (PCs) and the computer network in the Fire/EMS Department.

1. If a problem with the PCs occurs, do not attempt to fix it yourself outside of general troubleshooting. Under no circumstances are you to take the computers apart as they are under warranty and any mishandling will invalidate the warranty. Complete the troubleshooting steps found on the following page. Upon completion of this process, if equipment is still inoperable, contact Information Management immediately at (301) 883-7183 or via email - PGFDInformationManagement@co.pg.md.us . Contact the Emergency Operations Center for issues that occur prior to 8:00 am and after 5:00 pm and weekends and holidays. The Operations Center number is (301) 583-2200. Please provide the Operations Center personnel with the following information:
    - Identify what station you're calling from and the problem.
    - Provide a contact person, and bar code of equipment that is malfunctioning.
2. Take precaution when using personal disks, ensure they're not infected with a virus. Be mindful of the latest viruses. The computer is equipped with a virus scan program, but not all viruses are caught. If you suspect the computer has a virus, please contact Information Management personnel.
3. All PCs will be placed in an area that is accessible to both the career and volunteer contingent of the Department.
4. Care should be taken to ensure that the PCs remain free of dust, dirt and diesel fumes.
5. The County has installed on the PCs the following software applications:
    A. Microsoft Word
    B. Microsoft Excel
    C. Microsoft Access
    D. Microsoft PowerPoint
    E. Microsoft Outlook
    F. PDSI Telestaff
    G. Fire RMS
6. No additional software is to be installed on the computers unless written permission is received from the Department's Information Management Division. There will be periodic audits of the PCs. Any unauthorized software will be removed immediately, without warning!
7. Each employee and member that uses the PCs must adhere to the County "Electronic Information Policy" and the "Electronic Mail Acceptable Use Standard".

Checking for Network Problems

The Network Infrastructure Equipment listed below represents what is currently installed in the majority of the County's Fire Stations & Battalion Sites.

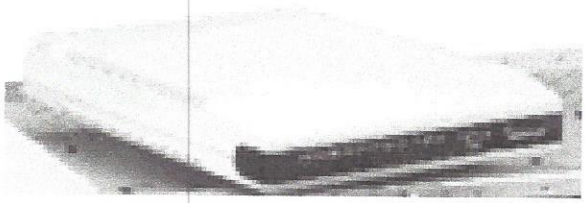
Equipment:

1. Cisco 2800 series Router
2. Comcast Router

The Comcast data line comes into our buildings via a coax cable connected to the Comcast router. The data line is then jumped via an Ethernet cable into the Cisco 2800 Router. All the equipment at the fire stations and Battalion sites are connected to the switching ports on the Cisco router via Ethernet cables. This equipment can be found in the black communication box at the fire stations and Battalion sites.

For the computers and printers to be connected to the network and be fully operational, the Cisco 2800 Router must be online at all times. If you notice any of the following signs indicating that the Router is down, please call the Information Management help desk immediately after confirming that the equipment is receiving electric power.

1. Inability to logon to the computer.
2. Inability to get on the internet
3. Inability to open the share drives
4. CAD printer will not print



PRINTER Equipment below is what currently is in operation at the majority of the Prince George's County's Fires Stations & Battalion Sites.

Tally ML9030, ML260, and HP Laser Jet Printers

1). Check Printer--- Verify for Ready or On Line in LED.
Make sure printer is connected to the Uninterruptible Power Supply (UPC) which is in the black communications cabinet, Verify that the power strip is ON.

Basic Printer Problem Trouble Shooting Possible Causes:

The Cable may be loose or defective.
The Printer may be displaying an error message

Basic Troubleshooting Procedures:

These basic-troubleshooting steps may resolve or more accurately diagnose numerous printer problems and can be used with most printers.

Perform a self-test on the printer by turning it off then back on -- It is important to insure that the printer will perform a self-test. This isolates the problem to something other than the operation of the printer itself.

Make sure that the network cable is connected to the printer and the printer is turned on.

Check the Printer to see if it is out of paper or not connected.

Check the paper in the printer to see if there is any jammed in the printer.

Make sure that the printer has not become disconnected or turned off.

If all the above steps do not resolve the problem, call IM help desk at 301-883-7183.

4.0 Fire/EMS Department Applications

4.1 Zoll Data Systems Records Management System (RMS) PDSI Telestaff/Webstaff

Section 3.5 will guide you through logging on to RMS, Telestaff and Webstaff. Detailed presentations on how to use these applications can be found on the Fire/EMS Department's intranet site as follows:

- Management Services/Information Management/Training Slides – FireRMS
- Management Services/Information Management/Training Slides – Telestaff

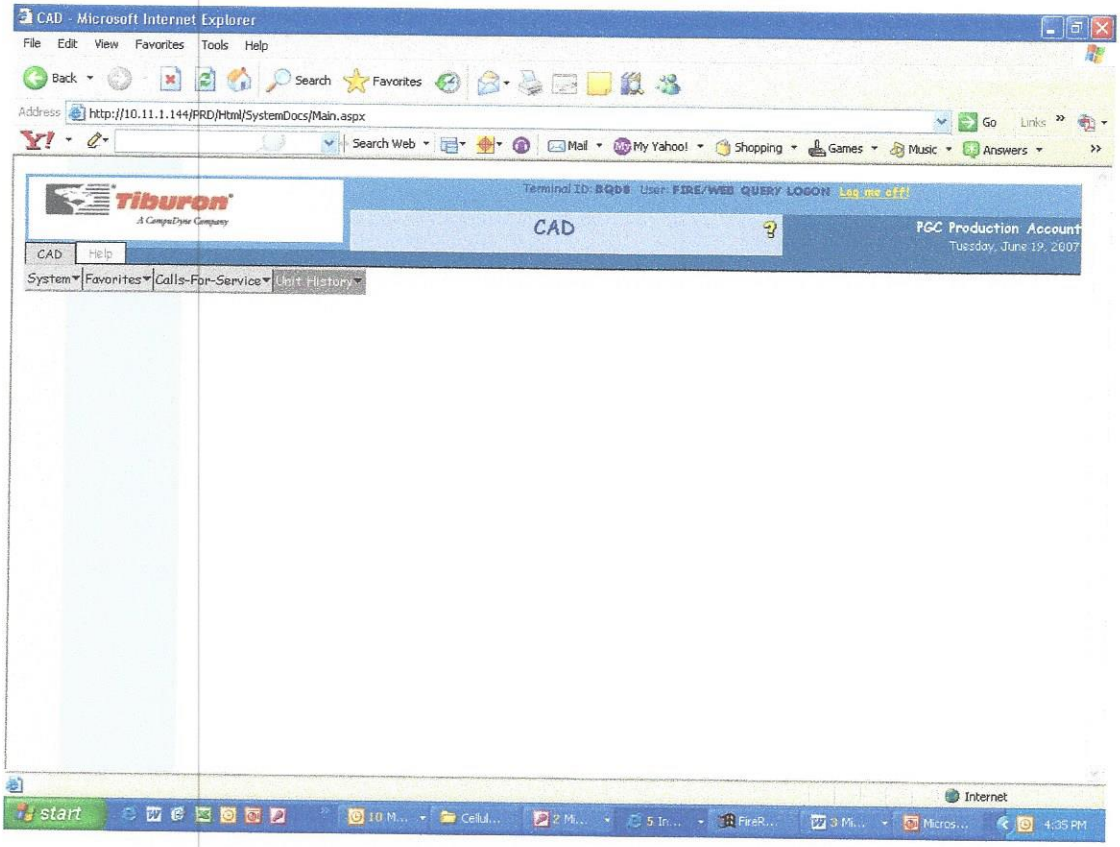
4.2 Computer Aided Dispatch (CAD) Web Query Instructions

The Tiburon Computer Aided Dispatch (CAD) WebQuery/2000 is a web browser based product used to query the CAD Records Management System/2000 for fire and EMS incidents.

The link to the CAD Web Query is http://10.11.1.144/prd

You cannot use the web browser until you have logged on to the Network (See section 3.5)

1. Position the cursor in the "User Name" field and enter your user name (FIRE) and password (Fire).
2. Click the *Log On* button.
3. A message appears that informs you if you have entered the user name or password incorrectly.
4. If a successful log on is processed, the desktop will be displayed.

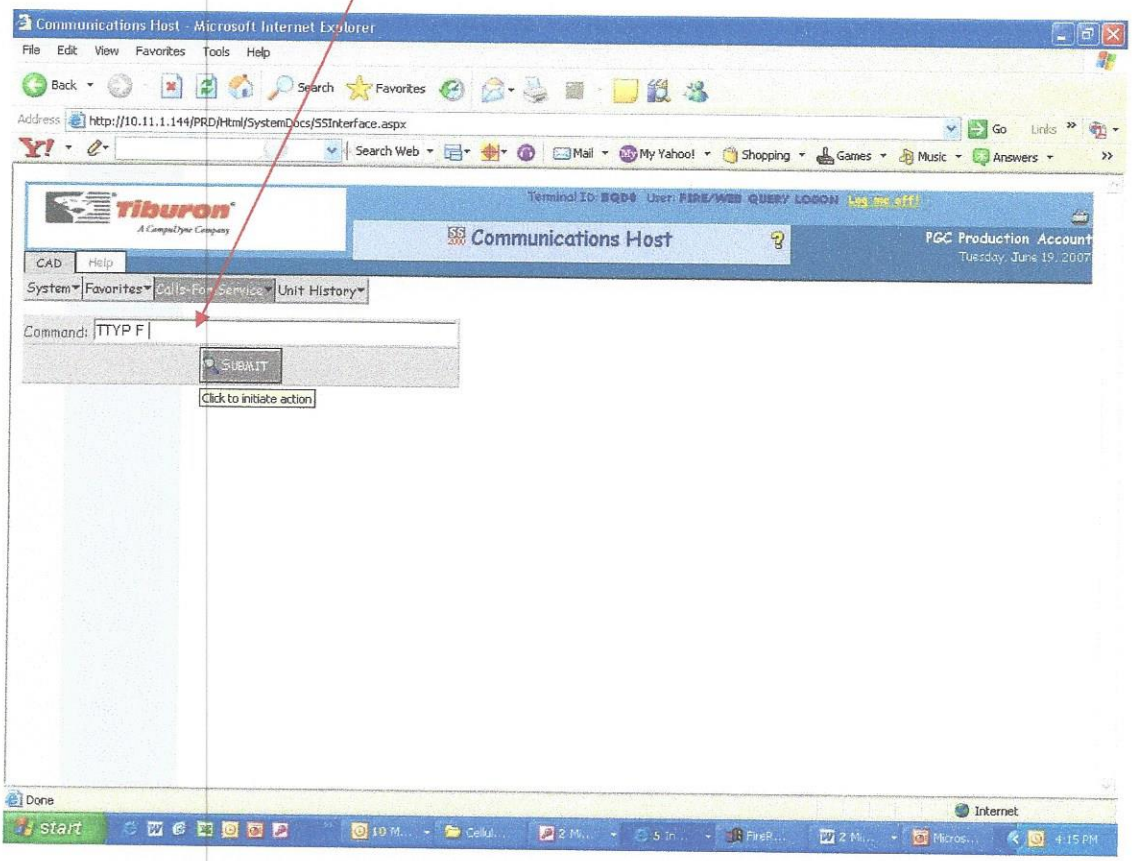


NOTE: When connecting to the browser, you may get a message related to downloading an ActiveX control. This control is required for starting the GUI applications from the menu. Because of this you may receive the following message when first connecting to the browser:

Your current security settings prohibit running ActiveX controls on this page. As a result, the page may not display correctly.

You need to change the security for your browser in order to allow the download and usage of this control. Contact Information Management if you need further assistance.

5. If you are logging into Web query for the first time, in order for the fire information to show you need to do the following:
    a. In the System drop down choose Communications Host
    b. In the Command box type TTYP F (there is a space before the F)
    c. Click submit
    d. A blue banner with OK should appear. If you are already in the Fire Department it will indicate "You are already agency PF"
    e. Bring up the Communications Host again
    f. Type in QIH
    g. Fire incidents should now be displayed
    h. Once this is done it will display fire calls until changed



6. Typing QIH (Query Incident History) in the Command line will give you a listing of all the fire and EMS calls for the day.
7. Typing QUH (Query Unit History) in the Command line will give a history of a particular unit.

8. Information Management is working with Public Safety Communications to get a list of all the commands that Fire/EMS Department personnel are authorized to use.

5.0 The Health Insurance Portability and Accountability Act

5.1 What is HIPAA?

Effective April 14, 2003, the Federal Government implemented legislation that ushered in the most significant changes in the health care industry since Medicare. This new legislation is known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As a provider of emergency medical services, the Prince George's County Fire/Emergency Medical Services (EMS) Department is a "covered entity" and is required to act in accordance with the administrative simplification standards of HIPAA.

5.2 The Fire/EMS Department's Responsibility as it pertains to HIPAA

The Fire/EMS Department's responsibility as it pertains to HIPAA is outlined in Division 3 – Chapter 5. The HIPAA General Order establishes guidelines to ensure that the Department is compliant with the Privacy Rule portion of the administrative simplification standard of HIPAA. Below is the notice that is to be given out to patients. Copies of the "Notice of Privacy Practices" should be stored on all apparatus and within station files for distribution to those that make a request. Personnel are permitted to distribute the "Notice of Privacy Practices" upon request.

5.3 Notice of Privacy Practices

THE PRINCE GEORGE'S COUNTY GOVERNMENT
Fire/EMS Department Headquarters

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

YOUR HEALTH INFORMATION RIGHTS

You have the following rights regarding the health information that Prince George's County Fire/Emergency Medical Services Department collects and maintains about you:

Right to Inspect and Copy: **You have the right to inspect and obtain a copy of your health information within 21 working days after you request disclosure. This request may include your medical, billing or health care payment information. It does not include information that is needed for civil, criminal, administrative actions or proceedings or psychotherapy notes. We may charge a fee for the costs of copying, mailing or other supplies associated with your request.**

Right to Amend: **If you feel that the health information the Prince George's County Fire/EMS Department has created about you is incorrect or incomplete, you may ask us to amend that information. The Prince George's County Fire/EMS Department may deny your request if you ask to amend information that: 1) was not created by the Prince**

George's County Fire/EMS Department; 2) is not part of the health information kept by Prince George's County Fire/EMS Department; 3) is not part of the information which you would be permitted to inspect or copy; or 4) the information is determined to be accurate and complete.

Right to Accounting of Health Information Releases: **You have the right to request a list of information releases that Prince George's County Fire/EMS Department has made of your health information during the 6 years before your request. The list will not include: 1) health information releases made for purposes of providing treatment to you, obtaining payment for services or releases made for administrative or operational purposes; 2) health information releases made for national security; 3) health information releases made to correctional institutions and other law enforcement custodial situations; 4) health information releases Prince George's County Fire/EMS Department has made based on your written authorization; 5) health information releases to persons who are involved in your care; or 6) health information releases made prior to April 16, 2003.**

Right to Request Restrictions: **You have the right to request a restriction or limitation of the health care information Prince George's County Fire/EMS Department uses or releases for treatment, payment or operational purposes. The Prince George's County Fire/EMS Department is not legally required to with agree the requested restriction or limitation.**
Right to Request Confidential Communication: **You have the right to request that we communicate with you about health care matters in a certain way or at a certain location. For example, you can request that we only contact you at work or by email. The Prince George's County Fire/EMS Department will accommodate all reasonable requests. To request confidential communications, you must specify how or where you wish to be contacted.**

Right to a Paper Copy of this Notice: **You have the right to request a paper copy of this notice from us at any time.**

All requests for inspecting, copying, amending, making restrictions, or obtaining an accounting of your health information must be made in writing to:

Prince George's County Fire/EMS Department
Information Management
9201 Basil Court, Suite 352
Largo, Maryland 20774

HOW PRINCE GEORGE'S COUNTY FIRE/EMS DEPARTMENT USES AND RELEASES HEALTH CARE INFORMATION

Your health information may be used and released by the Prince George's County Fire/EMS Department for the purposes of providing treatment to you, obtaining payment for services, for administrative and operational purposes and to evaluate the quality of the services that you receive. Prince George's County Fire/EMS Department provides a wide

range and variety of prehospital health care to the people in Maryland. For this reason, not all types of uses and releases can be described in this document. We have listed some common examples of permitted uses and releases below.

For Treatment: **Caregivers, such as Emergency Medical Services (EMS) providers, nurses, doctors, therapists and social workers may use your health information, both oral and written, to determine your plan of care. EMS providers may transmit your health care information by radio or telephone or in writing in order to assist in your care.**

For Payment: **Prince George's County Fire/EMS Department may release information about you to your health plan or health insurance carrier to obtain payment for services. For example, we may need to give your health plan information about a transport that you or your child received so your health plan will pay us or reimburse you for treatment or services the Prince George's County Fire/EMS Department provided. We may also share your information, when appropriate, with other government programs such as Workers' Compensation, Medicaid, or Medicare in order to coordinate your benefits and payments.**

For Health Care Operations: **Prince George's County Fire/EMS Department may use and release information about you to ensure that the services and benefits provided to you are appropriate and are high quality. For example, we may use your information to evaluate our treatment and service programs or to evaluate the services of other EMS providers in our jurisdiction. We may combine health information about many individuals to research health trends, to determine what services and programs should be offered, or whether new treatments or services are useful. We may share your health information with billing services who perform functions on behalf of Prince George's County Fire/EMS Department. We require that our billing services abide by the same level of confidentiality and security as we do when handling your health information.**

To Government Agencies Providing Benefits or Services: **Prince George's County Fire/EMS Department may release your health information to government agencies that are providing you benefits or services when the information is necessary for you to receive those benefits and services.**

For Public Health: **Prince George's County Fire/EMS Department may release your health information to public health agencies, subject to the provisions of applicable state and federal law, for the following kinds of activities:**

- **(i) To prevent or control disease, injury or disability or to keep vital statistics records such as births and deaths**
- **(ii) To notify social service agencies that are authorized by law to receive reports of abuse, neglect or domestic violence;**
- **(iii) To report reactions to medications or problems with products to the Food and Drug Administration (FDA).**

For Health Oversight Activities: Prince George's County Fire/EMS Department may share your health information with State and local agencies for oversight activities as required by law. Examples of these oversight activities include audits, civil, administrative, or criminal

investigations; inspections; licensure/certification or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The emergency medical care system and the health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

For Law Enforcement: **Prince George's County Fire/EMS Department may release health information to a law enforcement official, subject to applicable federal and state law and regulations, for purposes that are required by law or in response to a court order or subpoena.**

For Research: **Prince George's County Fire/EMS Department may release your health information for research projects that have been reviewed and approved by an institutional review board or privacy board to ensure the continued privacy and protection of the health information.**

Lawsuits and Disputes: **If you are involved in a lawsuit or a dispute, Prince George's County Fire/EMS Department may release health information about you in response to a court or administrative order. We may also release health information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.**

To Coroners, Medical Examiners and Funeral Directors: **Prince George's County Fire/EMS Department may release health information to a coroner, medical examiner or funeral director, as necessary to carry out duties as authorized by law.**

To Avert A Serious Threat to Health or Safety: **Prince George's County Fire/EMS Department may release your health information if it is necessary to prevent a serious threat to your health and safety or to the health and safety of the public or another person.**

For National Security: **Prince George's County Fire/EMS Department may release your heath information to authorized federal officials or other authorized persons for purposes of national security.**

To a Correctional Institution: **If you are an inmate of a correctional institution or under the custody of a law enforcement officer, Prince George's County Fire/EMS Department may release your health information to the correctional institution or law enforcement officer.**

The information released must be necessary for the institution to provide you with health care, protect your health and safety or the health and safety of others, or for the safety and security of the correctional institution.

To the Military: **If you are a veteran or a current member of the armed forces, Prince George's County Fire/EMS Department may release your health information as required by military command or veteran administration authorities.**

To Individuals Involved In Your Care: **Prince George's County Fire/EMS Department may release your health information to a family member, other relative, friend or other person whom you have identified to be involved in your health care or the payment of your health care.**

To Family: **Prince George's County Fire/EMS Department may use your information to notify a family member, a personal representative or a person responsible for your care, of your location, general condition or death.**

To Disaster Relief Agencies: **Prince George's County Fire/EMS Department may release your health information to an agency authorized by law to assist in disaster relief efforts.**

PRINCE GEORGE'S COUNTY FIRE/EMS DEPARTMENT'S REQUIREMENTS

Prince George's County Fire/EMS Department is required by state and federal law to maintain the privacy of your health information. We are required to give you this notice of our legal duties and privacy practices with respect to the health information that Prince George's County Fire/EMS Department collects and maintains about you. We are required to follow the terms of this notice.

This notice describes and gives some examples of the permitted ways that your health information may be used or released. Release of your information outside of the boundaries of Prince George's County Fire/EMS Department-related treatment, payment or operations, or as otherwise permitted by State or Federal law, will be made *only* with your specific written authorization. You may revoke specific authorizations to release your information, in writing, at any time. If you revoke an authorization, we will no longer release your health information to the authorized recipient(s), except to the extent that Prince George's County Fire/EMS Department has already used or released that information in reliance of the original authorization.

Prince George's County Fire/EMS Department reserves the right to revise this notice. We reserve the right to make the revised notice effective for the health information we already maintain about you, as well as any information we create or receive in the future. We will provide a copy of our revised notice to you upon request. We will post a copy of the current notice on our website at http://www.co.pg.md.us/Government/PublicSafety/Fire-EMS/index.asp, and at all Prince George's County Fire/EMS Department fire stations. In addition, you may ask for a copy of our current notice of privacy practices anytime you visit one of our fire stations.

FOR MORE INFORMATION OR TO REPORT A PROBLEM

If you believe your privacy rights have been violated, you may file a complaint with any or all of the agencies listed below. There will be no penalty or retaliation for filing a complaint.

Office of Civil Rights
Phone: 866-OCR-PRIV (866-627-7748) or
866-788-4989 TTY.

Secretary of Health and Human Services
200 Independence Ave., SW,
Washington, D.C. 20201
Toll Free Phone: 877-696-6775

Privacy Officer

Prince George's County Fire/EMS Department
Information Management
9201 Basil Court, Suite 352
Largo, Maryland 20774
301-883-7183

Secretary of Health and Human Services
200 Independence Ave., SW,
Washington, D.C. 20201
Toll Free Phone: 877-696-6775

To obtain more information about Prince George's County Fire/EMS Department's privacy practices, to receive additional copies of this notice or to receive request forms to access or amend health information, please contact:

Prince George's County Fire/EMS Department
Information Management
9201 Basil Court, Suite 352
Largo, MD 20774

6.0 County Cellular Phone Policy

The Fire/Emergency Medical Services Department current cellular telephone provider is Verizon Wireless. In an effort to become more efficient in our cellular telephone use below are the guidelines the will govern the use of the phone that you are being issued:

1. The phone that you have been assigned includes the following in its plan:
    a. 600 Anytime Minutes. These minutes are part of an overall pool of approximately 70,000 minutes.
    b. Unlimited nights (9:00pm – 6:00am)
    c. Unlimited weekends (9:00pm Friday – 6:00am Monday)
    d. Free Verizon Mobile to Mobile
    e. Unlimited data and text allowance.
2. ***Cell phones are for business use only***. It is understood that on occasion, you may need to use the phone for personal reasons. However, please be advised that you will be responsible for reimbursing the County for any overages that you may incur above the monthly allowable minutes. The Manager of Information Management will be monitoring the cell phone usage on a monthly basis.
3. Included with your phone are a wall charger, car charger, stereo headset, and phone case. If you have a Be advised that you will be responsible for these items and their replacement if they are lost or damaged.
4. The cell phone is covered under a one (1) year warranty. However, it is not covered for water damage. After the warranty period has expired you will be responsible for the repair and/or replacement of the cell phone as well as any loss or damage not covered during the warranty period. . Information Management personnel will assist you with the process of replacing the phone as needed during both the warranty period and after the warranty period has expired.

7.0 Requesting Assistance from Information Management

What Information Management Provides

The Information Management Team provides various types of assistance to Department personnel. By submitting the proper request forms in a timely manner IM personnel will provide support in the following areas:

- Technical Assistance (Included conference calling setup)
- Software Support
- Statistical Information
- Equipment Relocation

If assistance is needed in any of the above referenced areas, email Information Management at PGFDInformationManagement@co.pg.md.us. Also, the following forms can be obtained via the Intranet under the Management Services Command.

7.1 Fire/EMS Department Information Management Software Support Request Form

Please use this form to request software support.

Name: _____

Date of Request: _____

Software Support Needed:

_____ **Microsoft Word**

_____ **Microsoft PowerPoint**

_____ **Microsoft Access**

_____ **Microsoft Excel**

_____ **Records Management System**

_____ **Telestaff**

_____ **Other (Please Specify)**_____

Request Details (Training Needed, Assistance with setting up spreadsheet, creating database, etc):

_____

_____

_____

_____

_____

Date Required by (if applicable):_____

Please Email completed form to pgfdinformationmanagement@co.pg.md.us

7.2 Fire/EMS Department Information Management Statistical Request Form

Please use this form to request the data, analysis or information you require.

Name: _____

Date of Request: _____

Request Details: _____

_____

_____

_____

_____

_____

_____

_____

- Be as specific as possible and **include some context around when you require the information by** if possible.
- Please be aware, on average requests are turned around within five (5) working days.
- Requests for information may be far more complex than they seem, so as much notice as possible is appreciated in order to try to schedule work appropriately.
- For more lengthy requests or supportive material, please create an attachment.

Date Required by: _____

Purpose of Request:

_____

Please Email completed form to pgfdinformationmanagement@co.pg.md.us

7.3 Fire/EMS Department Information Management Technical Assistance Form

IMPORTANT: You must return this form at least five (5) days before your event. Failure to do so may result in a lack of technical support.

This form will be used to set up your event, so the more information and detail you give us, the better prepared our staff will be.

Date of Event: _____

Location of Event: _____

Time of Event: _____

Approximate End Time (if Information Management personnel are needed):_____

Contact Name and Phone Number: _____

Technical Needs: (check all that apply)

___ Conference Call Setup
- Title of the Conference _____
- Duration of the Conference _____
- Number of Participants _____

___ LCD Projector

___ Laptop PC

___ Software Applications needed

___ Network Connectivity (Wired)

___ Network Connectivity (Wireless)

Any Other Requirements:

Please Email completed form to pgfdinformationmanagement@co.pg.md.us

7.4 Fire/EMS Department
Equipment Relocation Procedure

Equipment Relocation

Information Management and the Office of Information Technology and Communications (OITC) are responsible for the installation, maintenance, and relocation of all computers, printers, communication equipment, VoIP phones, cellular phones and scanners. Fire/EMS Department personnel relocating or temporarily moving during construction or moving to another work area must communicate the details of the move to Information Management (IMD) prior to the move. Under no circumstance, should any computer equipment or peripherals be moved without properly notifying Information Management via the attached Relocation Form. Since for the most part computers and related peripherals are assigned to the position or station not the person, Information Management will make the determination if the equipment needs to be relocated. If it is determined that adequate equipment is available at the new location the Information Management staff will work with personnel to ensure all the files and programs are available at the new assignment location.

7.5 Fire/EMS Department Information Management Equipment Relocation Form

Reason for Relocation:	
Current Assignment and Location	
Date of Request:	Command/Division:
Name:	Room:
Building/Station:	Phone #
New Assignment and Location	
Move Date:	Command/Division:
Name:	Room:
Building/Station:	Phone #

Item #	Barcode	Description	Serial #
1			
2			
3			
4			
5			
6			

Does computer have any special software installed?
If yes, please list

Please Email completed form to pgfdinformationmanagement@co.pg.md.us