THE FOLLOWING EXHIBITS MUST BE READ BY ALL MEMBERS BEFORE SIGNING A MEMBER AGREEMENT

Exhibit A-1
Password Policy

1.0 Overview
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Baltimore County's entire network. As such, all Baltimore County employees (including contractors and vendors with access to Baltimore County systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1.1 Scope
This policy applies to all Baltimore County employees, contractors, vendors and agents that require access to Baltimore County network or systems. This includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Baltimore County facility, has access to the Baltimore County network, or stores any non-public Baltimore County information.

1.2 Policy
1.2.1 General
While some systems may require passwords to be changed more frequently, it is the user's responsibility to ensure that all passwords are changed at least quarterly.
User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
Passwords must not be inserted into email messages or other forms of electronic communication.
All user-level and system-level passwords must conform to the guidelines described below.

The initial passwords issued by a security administrator must be valid only for the involved user's first on-line session. At that time, the user must choose another password before any other work can be done.
Where possible, after three unsuccessful attempts to enter a password, the system administrator must revoke the involved User ID until reset.
Passwords must always be encrypted when held in storage or when transmitted over networks.
Actual compromising of systems or even suspicion of compromise requires all system passwords be changed immediately on all impacted systems.
To receive a reset of your password, you must provide a PIN number (last four digits of your social security number) in order to identify yourself. Non-County employees who have access to County systems will be asked to provide this information when receiving access to County systems.

1.2.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Baltimore County. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Passwords should be easy to remember but difficult to guess. Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

The password contains less than eight characters
The password is a word found in a dictionary (English or foreign)
The password is a common usage word such as:
Names of family, pets, friends, co-workers, fantasy characters, etc.
Computer terms and names, commands, sites, companies, hardware, software.
The words "Baltimore County", "balto", "county" or any derivation.
Birthdays and other personal information such as addresses and phone numbers.
Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
Any of the above spelled backwards
Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

Contain both upper and lower case characters (e.g., a-z, A-Z)
Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
Are at least eight alphanumeric characters long.
Are not a word in any language, slang, dialect, jargon, etc.
Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for Baltimore County accounts as for other non-Baltimore County access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Baltimore County access needs.
Do not share Baltimore County passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Baltimore County information.

Here is a list of "dont's":

Don't reveal a password over the phone to ANYONE
Don't reveal a password in an email message
Don't reveal a password to the boss
Don't talk about a password in front of others
Don't hint at the format of a password (e.g., "my family name")
Don't reveal a password on questionnaires or security forms
Don't share a password with family members
Don't reveal a password to co-workers while on vacation
If someone demands a password, refer them to this document or have them call the director's office of Baltimore County's Office of Information Technology (OIT) 410-887-3223.
Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).
Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
If an account or password is suspected of compromise, report the incident to the OIT Helpdesk (410-887-8200) immediately and change all passwords.

C. Use of Passwords for Remote Access Users

Access to the Baltimore County Networks via remote access is to be controlled using password authentication. (See Remote Access Policy). Violation of this policy may result in the removal of the Baltimore County equipment and termination of access to County network and systems. Additionally, violation of this policy may constitute contract breach and result in further legal action. Any Baltimore County employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

1.4 Definitions

Password

A sequence of characters that one must input to gain access to a file, application, or computer system.

Remote access

Any access to Baltimore County's network through a non-Baltimore County controlled network, device, or medium.

Strong password

Contain both upper and lower case characters (e.g., a-z, A-Z)
Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~ =\`{}[]:";'<>?,./)
Are at least eight alphanumeric characters long.
Are not a word in any language, slang, dialect, jargon, etc.
Are not based on personal information, names of family, etc.

1.5 Revision History

Revised December 29, 2003

Exhibit A-2
Remote Access Policy

2.0 Overview

The purpose of this policy is to define standards for connecting to Baltimore County's network from any host outside of the Baltimore County Local Area Network (LAN). These standards are designed to minimize the potential exposure to Baltimore County from damages, which may result from unauthorized use of Baltimore County resources.

2.1 Scope

A Baltimore County Agent is defined as any Baltimore County employee, contractor, vendor, agent or other entity that requires access to Baltimore County networks or systems. This policy applies to Baltimore County Agent's remote access connections used to do work on behalf of Baltimore County. The policy does not apply to the use of the County's public web sites or Internet-based GroupWise Webaccess.
Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, and cable modems.

2.2 Policy

2.2.1 General

1. Dial Up Access to the Baltimore County network must be obtained by filling out a "Dial Up Request" form located on the Intranet under OIT Forms.
2. The Baltimore County Agent is responsible to ensure that individuals under their direction or control do not violate any Baltimore County policies, do not perform illegal activities, and do not use the access for outside business interests. The Baltimore County Agent bears responsibility for the consequences should the access be misused.
3. Additionally, a Baltimore County Agent that observes a violation of this or any other Baltimore County Information Technology Policy is responsible for reporting that violation to the Baltimore County Office of Information Technology (410-887-8200). Failure to report such activity is a violation of this policy as considered in Section 2.3 Enforcement of this Policy.
4. Please review the Electronic Communications policy for details of acceptable use of County resources.

2.2.2 Requirements

1. Secure remote access must be strictly controlled. Firewalls attached by Baltimore County's Office of Information Technology (OIT) cannot be modified and must remain properly connected at all times.
2. At no time should any Baltimore County Agent provide his or her login or email password to anyone, not even family members. (See Password Policy)
3. Baltimore County Agents and contractors with remote access privileges must ensure that their computer or workstation, which is remotely connected to Baltimore County's network, is not connected to any other network at the same time.
4. Reconfiguration of a user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
5. Hardware and security configurations installed by Baltimore County may not be modified or removed by the agent without prior written approval of the Network & Systems Manager or Director of OIT.
6. Non-standard hardware and security configurations must be approved by the Network & Systems Manager or Director of OIT.
7. All hosts, including personal computers, that are connected to Baltimore County internal networks via remote access technologies must use the most up-to-date antivirus software and must be regularly scanned for viruses. (See Anti-Virus Policy)
8. Personal equipment that is used to connect to Baltimore County's networks must meet the requirements of Baltimore County-owned equipment for remote access.
9. Organizations or individuals that wish to implement non-standard Remote Access solutions to the Baltimore County production network must obtain prior approval the Director of OIT.
10. At no time should network logical or physical configuration be modified in any way that makes the County policy enforcement point (firewall, etc) ineffective at enforcing the prescribed policy.
11. At no time should any software, hardware solution, or hardware configuration be implemented which circumvents firewall policy.

12. At no time should any DHCP or BOOTP server be implemented in the same broadcast domain as the Count y-issued devices (PC, firewall, etc) or any hardware or software feature implemented to proxy, forward, or relay traffic related to these services out to other broadcast domains.
13. At no time should a wireless access point (WAP) or "ad hoc" mode client(s) be implemented behind the County issued firewall (i.e. between the firewall and the PC accessing County systems).

14. At no time should software be installed or used on systems behind the county firewalls that allow for the tunneling of other protocols (i.e. between the firewall and the PC accessing County systems).
15. At no time should the Baltimore County Agent use any network service that is not enumerated in the attached Approved Services Addendum prior written approval of the Network & Systems Manager or Director of OIT.

2.3 Enforcement
Violation of this policy may result in the removal of the Baltimore County equipment and termination of access to County network and systems. Additionally, violation of this policy may constitute contract breach and result in further legal action. Any Baltimore County employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. The Baltimore County Agent understands and hereby acknowledges the County's right to maintain logs, monitor activities, install and maintain router and firewall hardware, perform physical inspections, and perform any other measures the County in its sole discretion may deem appropriate, all without notice, to ensure that the terms and conditions of this Agreement are maintained and enforced.

2.4 Definitions
Baltimore County Agent A Baltimore County Agent is defined as any Baltimore County employee, contractor, vendor, agent or other entity that requires access to Baltimore County networks or systems.
BOOTP BOOTP (Bootstrap Protocol) is a protocol that lets a network user be automatically configured (receive an IP address) and have an operating system booted (initiated) without user involvement.
Broadcast Domain A broadcast domain is a restricted area in which information can be transmitted for all devices in the domain to receive. More specifically, Ethernet LANs are broadcast domains.
Cable Modem Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
DHCP Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network.

Dial-in Modem A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Baltimore County-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Baltimore County and an ISP, depending on packet destination.
Digital Subscriber Line (DSL) DSL is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
ISDN There are two flavors of Integrated Services Digital Network or ISDN:
BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Proxy In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service.
Remote Access Any access to Baltimore County's network through a non-Baltimore County controlled network, device, or medium.
Split-tunneling Simultaneous direct access to a non-Baltimore County network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Baltimore County's network via a VPN tunnel.
VPN Virtual Private Network VPN is a method for accessing a remote network via "tunneling" through the Internet.

2.5 Revision History *Revised December 29, 2003*

Approved Services Addendum

The following data transmission services are approved for use by PCs that remotely access Baltimore County networks or systems. If you have any questions or require clarification regarding this list, contact the Baltimore County Office of Information Technology, Manager of Network and Systems Unit at 410-887-4176.

Definitions
Ingress traffic - inbound traffic stream initiated by external source. Note ALL ingress traffic ends in the County's DMZ (i.e. the area between the County's internal and external firewalls) either at a public hosts or a proxy firewall. IPSEC tunnels from remote sites terminate at the towson1 head-end and the tunneled traffic passes through the proxy firewalls to the internal destinations.

Egress traffic - outbound traffic and for the purposes of this document, the return ingress traffic associated with the outbound communication.
Approved Services Egress (proxied outbound)
· http
· https
· ftp
· telnet
· ntp
· ipsec (back to Baltimore County network only)
· AIM*
· MSN Windows messenger*
*These use socks communications
Ingress (inbound)
· http
· https
· ftp (passive)
· ipsec

Exhibit A-3
AntiVirus Policy

3.0 Overview
The purpose of this policy is to define standards for preventing the introduction of viruses or other malicious software into the County network and its connected devices. Prevention is achieved through the use of antivirus software and best practices.

3.1 Scope
This policy applies to all Baltimore County employees, contractors, vendors and agents that use a device that connects or is connected to the Baltimore County network or systems.

3.2 Policy
3.2.1 General Prevention
The department, agency or IT administrator will install antivirus software approved by OIT on all servers to limit the spread of viruses within the network. Workstations will have memory resident antivirus software installed and configured to scan data as it enters the computer. Programs will not be executed, nor files opened by applications prone to macro viruses, without prior scanning for viruses.
All incoming mail and files received from across a network must be scanned for viruses as they are received and prior to delivery to e-mail boxes. Virus checking will be performed, where applicable, at firewalls that control access to networks. This allows for centralized virus scanning for the entire department or agency.

Virus scanning definitions shall be updated at least on a **weekly** basis to remain current with the latest virus signatures. It is important for employees to immediately inform the Office of Information Technology's Help Desk at 410-887-8200, of any suspected or actual virus infections. The IT administrator shall immediately disconnect a computer that is infected or thought to be infected from networks and complete a full clean of the virus to reduce risk of spreading.

3.2.2 Antivirus Guidelines

County-owned devices must always run County standard, supported anti virus software that is configured to auto update or is updated manually at least weekly. Any non-County-owned devices that connect with the County network in any manner must run updated commercial antivirus software.
NEVER open any files or macros attached to e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
Delete spam, chain, and other junk e-mail without forwarding to others.
Never download files from unknown or suspicious sources.
Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
Always scan a floppy diskette from an unknown source for viruses before using it.
Backup critical data and system configurations on a regular basis and store the data in a safe place

3.3 Enforcement

Violation of this policy may result in the removal of the Baltimore County equipment and termination of access to County network and systems. Additionally, violation of this policy may constitute contract breach and result in further legal action. Any Baltimore County employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.4 Definitions

virus A virus is a manmade program or piece of code that replicates itself repeatedly and causes an unexpected, usually negative, event.
antivirus software Software installed on a computer that is used to find and remove viruses.
Hoax Deliberate or unintentional e-mail messages warning people about a virus or other malicious software program that doesn't really exist.
spam e-mail Unsolicited e-mail (or news postings) pushing a point or product.
chain e-mail Chain e-mail is also a form of spam in that it is unsolicited. However, chain e-mail is often received from an acquaintance. The recipient of the e-mail is strongly pressured to keep the chain of e-mails going.
junk e-mail Junk e-mail is useless or non-business related e-mails similar to spam but could also come from an acquaintance.