INFORMATION SYSTEMS SECURITY POLICY

Scope of Security

Definition of Security

Bay Aging defines security as "the state of being free from unacceptable risk." The risk concerns the following categories of losses:

- Confidentiality of information – this refers to the concerns of privacy of personal and corporate information, including issues of copyright.
- Integrity of data – this refers to the accuracy of data. Loss of data integrity can have an extremely negative impact upon the Agency.
- Protection of assets – this should include:
  - Computer and peripheral equipment
  - Communications equipment
  - Computing and communication premises
  - Power, water, environmental controls, and communication utilities
  - Supplies and data storage material
  - System software (computer programs) and documentation
  - Application software and documentation
  - Information
- Efficient and appropriate use – this ensures that Information Systems resources are used for the purpose for which they were intended and in a manner that does not interfere with the rights of others.
- System availability – this area of concern is with the full functionality of systems.
- The potential causes of these losses are termed "threats." These threats may be human or non-human, natural, accidental, or deliberate.

Domains of Security

This policy specifically addresses the following domains of security:

- Computer system security: CPU, peripherals, and operating systems, including data security.
- Physical Security: The premises occupied by the Information Systems personnel and equipment.
- Operational Security: Environment control, power equipment, and operation activities.

- Procedural security by Information Systems, vendor, management personnel, as well as end users.

- Communication security: Communications equipment, personnel, transmission paths, and adjacent areas.

Reasons for Security

There are many reasons for Information System security:

- Confidentiality of information is mandated by reputation protection, common law, formal statute, explicit agreement, or convention. Different classes of information warrant different degrees of confidentiality. Bay Aging's Privacy of Customer Information Guidelines for Employees defines the Agency's two classes of information: confidential and non-confidential.

- The hardware and software components that constitute Bay Aging's Information Systems assets represent a sizable monetary investment that must be protected. The same is true for the information stored in its computer systems, some of which may have taken huge resources to generate.

- The use of the Agency's assets in a manner contrary to the purpose for which they were intended represents a misallocation of valuable organizational resources, and possibly a danger to its reputation or a violation of the law.

- Finally, proper functionality of Information Systems is required for the efficient operation of Bay Aging. Many systems are of paramount importance to the mission of the Agency.

Roles and Responsibilities

Policy Management

The Information Systems Security Policy of Bay Aging is of such vital importance that its approval is vested with the Board of Directors.

Advice and opinions in the Policy may be provided by:

- IT Steering Committee comprised of Senior Management.
- Computer consulting firm and third party service providers
- Auditors and other independent reviewers

Formulation and maintenance of the policy is the responsibility of the Management Information Systems Director.

Policy Implementation

Each staff member of Bay Aging is responsible for understanding and adhering to all Information Systems policies. Security of each system will be the responsibility of that system's custodian.

Custodians

The System Security/Network Administration will be the responsibility of the Management Information Systems (MIS) Director.

The Information Technology (IT) Department is the custodian of all strategic system platforms, the strategic communications systems, and all facilities where computer equipment is operated.

The IT Department and each department as appropriate, shares in the custodian duties of the strategic systems under their management control.

Individual staff members and the IT Department share in the custodian duties of desktop systems.

Individuals

All employees of Bay Aging must observe the following standards for use of Information System resources and systems:

- Every employee will operate under the provisions of Bay Aging's Microcomputer/Network Policy.
- Every employee must adhere to Bay Aging's Electronic Communications Policy.
- Every employee must be responsible for the proper care and use of Information Systems resources under their direct control.

Procedures, Standards and Guidelines

Procedures (step by step instructions for completing a specific task or function), standards (mandatory system or process requirements) and guidelines (suggestions or recommendations for a system or process) are published as part of this policy or subsequent to this policy to assist end-users and system custodians to meet their Information systems security responsibilities. Procedures are issued to support and implement the Policy. In addition, standards and guidelines are provided to facilitate and define the Policy.

Availability

The Information Systems Security Policy is accessible to all members of the Bay Aging staff via online access to the Agency's Intranet. All users of Bay Aging's Information Systems resources should be familiar with relevant sections of the policy.

Changes

This Information Systems Security Policy is a "living" document that will be altered as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers, etc. The organization's IT Committee must approve all changes.

Strategic Systems Platforms

Definition of Strategic Systems

Strategic systems are defined as those computer systems that are critical to the operation of Bay Aging. Such computer systems may be owned and operated by Bay Aging, or they may be owned and operated by another company with whom Bay Aging has established a business relationship. The following components comprise Bay Aging's strategic systems:

Four Windows 2003 File Servers:

- PowerEdge
- Exchange
- PE2970l
- 00Backup01

Physical Security

Bay Aging recognizes that its strategic systems, in addition to any other systems that contain confidential information, require a higher degree of physical security than is provided for other business operations. Computer equipment and network resources must be physically protected from damage, theft, or other harm due to environmental hazards (e.g., fire, flood, etc.). Hardware and software must be properly maintained and protected to ensure that they function appropriately and can be serviced or replaced according to licenses and agreements. The following standards of physical security for all strategic systems and systems containing confidential information must be met:

- The premises must be physically strong and reasonably free from risk of damage by water, fire, vibration, dust, and environmental hazards.

- Air temperature and humidity must be controlled within acceptable operating limits.

- Backup electrical power, such as that from an uninterruptible power supply (UPS) or generator, must be available to provide the following:

    - A minimum of 30 minutes on base and 60 minutes of operation on battery packs in the event of a power failure.
    - Adequate protection from power surges and sags.
    - "Power Shute" triggers an orderly shutdown of affected systems 10 minutes before the UPS batteries are depleted.

The primary location for most of the strategic systems at Bay Aging is at the company's

Data Center located at 5306 Old Virginia Street, Urbanna, Virginia. Power protection is provided by a series of Uninterruptible Power Supplies (UPSs).

It is expected that strategic systems not under the direct control of Bay Aging will adhere to similar standards as those set by the Agency.. Vendor relationships should not be established with vendors that do not adhere to such standards. Additionally, contracts with vendors should contain some verbiage addressing physical access of the strategic systems located at their offices. Failure to adhere to such standards should be considered a breach of contract.

Physical Access

Strategic systems located at Bay Aging are located in a specifically designated secure area. Access to this area is restricted to authorized personnel from the IT Department and the Network Consulting Staff. All other access by other individuals, whether Bay Aging employees or not, must be granted by an authorized person and documented on the Server Room Visitor's Log. External doors to the designated area must remain locked. External windows must be secured so as not to allow unauthorized access.

It is expected that strategic systems not under the direct control of Bay Aging, such as those operated by vendors of the Agency, will adhere to similar standards as the Agency. Relationships should not be established with vendors that do not adhere to such standards.

User Access

It is the responsibility of the Network Administrator to set security parameters and user access. The network facilitates electronic communication and information sharing within the Agency (shared file access and internal email) and outside the Agency (internet access and external email). To ensure the security, reliability and efficiency of the network, access to strategic systems (network, email and core processor) is granted under the following conditions:

- Whenever notified by Human Resources that a new employee has been hired and where they will be placed in the organization.

- Confirm with Department head where new employee is assigned as to the duties of the employee.

- The access level assigned to the new employee must be no higher than specified by the Department Head.

- Each user must be uniquely identified, for individual accountability, by a user identifier (user ID) associated only with that individual.

- Upon initial login, the user will be required to select a password that meets established password criteria for the system.

- Reset user access level when changes in job responsibilities occur.

- The above requests will be submitted to the Network Administrator on a New Employee Information System Access Checklist with proper authorization.

- Should an employee's duties change, access changes should be submitted to the Network Administrator on an Employee Permission Change Request.

Access to strategic systems will be removed under the following conditions:

- Upon termination of employment a request should be submitted to the Network Administrator on an Employee Separation/Termination Checklist by Human Resources.

- When requested by a member of the senior management of the Agency.

Fire Detection and Control

The designated area(s) for the location of strategic equipment must be protected by fire detection and suppression equipment. Fire suppression equipment should be of such a nature that it would not harm computer equipment. If smoke is detected by the smoke detectors an alarm will sound. It also transmits a signal to the building's fire alarm panel that notifies the Fire Department. The fire Department is located less than 2 blocks away.

Data Integrity

Daily backups of all strategic systems will be conducted to minimize data loss in the event of a system failure or disaster situation. The backup strategy must minimally allow for a five-day rotation of complete daily backups. Daily backups must be stored in a secure, fireproof environment. At no time should all backup copies of any strategic system reside at a single location. Validation of backup media should be conducted on a periodic basis (at least quarterly) to ensure proper operation.

The daily tapes will be labeled Monday through Thursday; the weekly tapes will be labeled weekly 1 through 5. The last business day of the month is labeled month-end. The daily tapes are stored in the Glen's office where they are secure and protected from fire. The weekly and monthly tapes are kept in the vault at the Warsaw Transit facility where they are secure and protected from fire. Password protected tapes will be sent via the Agency's courier to the designated locations. An inventory of all backup tapes in existence and their current disposition will be maintained by the IT Department. Year-end tapes are retained permanently.

Password Controls

Each strategic system should incorporate a comprehensive password control strategy. The following criteria should be met:

- All passwords must be complex in nature; they must be at least eight characters in length. They must contain three of the following four criteria, upper case letter, lower case letter, number or symbol.

- Passwords must be changed every 90 days. An employee may elect to change their password at any time, but if a password is not changed within 90 days, the system will force a password change.

- All passwords are suppressed from all output.

- There are no restrictions on repeating characters; however, the password must contain some change.

- Passwords cannot be reused.

- Repeated access attempts may indicate an effort to gain unauthorized access. When the limit of three attempts is reached, the user ID must be suspended. Reactivation must be performed by the Network Administrator..

Virus and Spyware Protection

The management of Bay Aging recognizes the threat computer viruses and spyware present to its computer systems and networks. As a result, several steps have been implemented to prevent infection:

- *User training* – Perhaps the best tool used to prevent a virus attack is stressing to users the importance of being cautious when opening email attachments and downloading anything from the Internet. Several times per year, an email message is distributed to all staff containing instructions regarding email and Internet downloads. Bay Aging's Microcomputer/Network Policy also addresses this area.

- *Network protection* – Bay Aging uses the Symantec Endpoint Protection Enterprise and MalwareBytes Enterprise to constantly check for viruses and spyware. Copies of this software have been installed on each file server. When any file is written to the network hard drive, the software scans the file for viruses and all internet activity is monitored for potential spyware. . A complete system scan is also conducted on each file server every night.

- *Desktop protection* – Bay Aging uses the Symantec Endpoint Protection and MalwareBytes products for individual desktop protection. Any file opened on the desktop system is scanned for viruses and all internet activity is monitored for potential spyware.

Virus and Spyware Signature Updates

The Agency Utility Server contains the console control software that is configured to automatically check the Symantec web site for virus definitions updates each night at midnight. If an update is available, it is downloaded and applied to all servers and workstations (no operator intervention is required). This method ensures automatic updating of the virus signatures as needed.

The Agency Utility Server also automatically checks the MalwareBytes website for spyware definition updates each night at midnight. If an update is available, it is downloaded and applied (no operator intervention is required). Each workstation checks the Utility server for updates every hour. If an update exists, it is distributed to the workstations. This method ensures automatic updating of the MalWareBytes signatures as needed.

Disaster Recovery

Each strategic system must have a viable disaster recovery plan, or a comprehensive disaster recovery plan must cover all strategic systems. The plan or plans should be tested on a periodic basis, at least annually.

Incident Response

Please refer to Agency's Incident Response Policy

Documentation

A copy of this policy will be distributed to each end-user department. End-user procedures should be created with these guidelines in mind.

Software Change Control

Definition

Software Change Control covers the control of all aspects of strategic systems software including the operating systems, compilers and utilities, third party and in-house developed applications, together with any command procedures and documentation to support and run them.

General Obligations

When software changes are required, it is essential that the changes are appropriately authorized and approved. Authorization for any software change must come from a member of the senior management, or the Management Information Systems Director. The only exception to this policy is for changes made to correct errors found in existing programs or procedures, or for "patches" to existing systems, such as Program Temporary Fixes (PTFs). Because it may not be convenient or advisable to delay applying such changes while waiting for approval, these types of changes can be made, but should be communicated to appropriate management personnel as soon as possible.

It is equally important that all software changes adhere to the following guidelines:

- Changes must not violate any other policies or procedures.
- Changes must be thoroughly tested.
- Changes must be sufficiently documented.
- Changes must be implemented as an appropriate time to reduce or eliminate disruption of customer activity, company workflow, and system operations.

Change Control Responsibilities

The following personnel have the responsibility for approving software changes:

- President
- Chief Operating Officer
- Any Senior Vice President

It is the responsibility of the IT Department to implement software changes.

Implementation of Vendor-Supplied Changes

Operating Systems

A review of all existing operating systems is conducted on at least a monthly basis by management and the Agency's Computer Consulting Firm to check for upgrades, releases, and patches that may recently have been made available. The Agency has patch management software that allows for monitoring and distribution on a timely basis (as Microsoft makes patches available). Initial implementation will be based on a cross section of representative workstations in the Agency. Given that there are no problems with this sample, full deployment will be initiated. This includes network operating systems, individual desktop operating systems and software, electronic mail operating systems, proxy server operating systems, network backup and recovery systems, and the host processing operating system.
In the event that a problem occurs that requires a patch to be installed outside the regularly scheduled times, the IT Department with the assistance of the Agency's Computer Consulting Firm should apply the necessary updates and notify Bay Aging management.

All upgrades, releases, and patches should be scheduled for implementation during off peak hours. All installations are performed under the direct supervision of the IT Department.

The IT Department with the assistance of the Agency's Computer Consulting Firm is also responsible for installing and updating desktop operating systems, office automation software products, electronic mail clients, network clients, browser software, various product clients, and other software used at the desktop level. These updates are performed on an as-needed basis. Every effort is made to maintain consistency throughout the network, but because of user preferences and the number of desktop systems in use, it is not possible to always have exactly the same levels of software on every computer. As new computers are introduced and older computers are reloaded, the latest software and software updates are always applied.

Documentation

Appropriate documentation must be provided for the following:

- Change control procedures – the procedures for implementing software changes should be fully documented and followed.
- Technical functions – a guide for the technical functionality of the software should be maintained by the IT Department.
- Operational functions – any operational instructions required should be available to the appropriate department.
- End-user functions – specific instructions for using the software should be available to the appropriate department.

Outsourcing and Vendor Management

Refer to the Agency's Outsourcing and Vendor Management Policy

Communications

Network Access Areas

Network access at Bay Aging can be divided into four major areas:

- Local Area Networks (LAN)
- Wide Area Networks (WAN)
- External access via modem
- Internet
-

Bay Aging has varying degrees of control over these areas of network access. In some cases, such as the LANs, the Agency has total control over the network operation. In the case of WANs, the Agency is responsible for maintaining the equipment necessary to process the data once it reaches each node (or location) of the WAN, but has no control over the data as it moves between the origination point and its destination over leased telecommunication lines. Bay Aging realizes it has no control over the Internet, and understands its challenge to protect its data that might be exchanged through this system.

Local Area Networks

Bay Aging uses the term Local Area Network or LAN to refer to a collection of computers physically located together and connected in such a way to allow them to share resources such as printers, disk drives, Internet, and fax connections. Bay Aging's network consists of seven LANs – one for each of its operational locations. Each local LAN uses the Ethernet 100BASE-T and/or Ethernet 1000BASE-T topologies. All cabling is Category 5. A combination of digital switches and hubs are used to segment the network.

When possible, servers are attached directly to switches to provide better network segmentation. All desktop computers, printers, and other end-user devices are attached to hubs, which are, in turn, attached to switches. Switches are generally located one per floor, if the environment has multiple floors. Fiber optic cables would be used to connect switches.

- LAN equipment is considered part of the strategic systems for Bay Aging. Standards for the physical security for all LAN equipment are the same as other strategic systems:

- The premises must be physically strong and reasonably free from risk of damage by water, fire, vibration, dust, and environmental hazards.

- Air temperature and humidity must be controlled within acceptable operating limits.

- Backup electrical power, such as that from an uninterruptible power supply (UPS) or generator, must be available to provide the following:

- A minimum of 30 minutes on base and 60 minutes of operation on battery packs in the event of a power failure.
- Adequate protection from power surges and sags.
- "Power Shute" triggers an orderly shutdown of affected systems 10 minutes before the UPS batteries are fully depleted.

The primary location of LAN equipment at Bay Aging is at the company's Data Center located at Data Center located at 5306 Old Virginia Street, Urbanna, Virginia.

LAN equipment located at Bay Aging is located in a specifically designated secure area. Access to this area is restricted to only authorize personnel from the IT Department and the Agency's Computer Consultant. All other access by other individuals, whether employees or not, must be granted by an authorized member of the personnel and documented on the Server Room Visitor's Log. External doors to the designated area must remain locked. External windows must be secured so as not to allow unauthorized access.

The designated area(s) for the location of LAN equipment must be protected by fire detection and suppression equipment. Fire suppression equipment should be of such a nature that it would not harm computer equipment. Fire extinguishers are available in the event of a small fire that can be easily handled by an individual.

Since the LAN is so dependent upon the operation of switches, hubs, and Category 5 cabling, redundant units of each are maintained by Bay Aging to replace any failed units. Backup units are tested annually to insure proper operation.

Wide Area Networks

Bay Aging uses the term *Wide Area Network* or WAN to refer to the interconnection of computers and local area networks over an extended area using leased telephone or cable data circuits. Bay Aging currently utilizes connections provided by MetroCast Cable to provide WAN connectivity between offices. Firewalls are installed at each office to connect the circuits.

Since Bay Aging's WAN does rely on leased telephone data circuits, there is a greater control risk associated with the WAN as compared to that associated with the LAN equipment used by the Agency. In recognition of this fact, Bay Aging has taken steps to ensure the integrity of the data that moves through the WAN is not compromised. Three key elements of network security are employed:

- User identification – each user of a system must be accurately and positively identified. Bay Aging uses password authentication on all of its systems for this purpose.

- Perimeter security – this element of security ensures that only authorized traffic passes through the network. Bay Aging uses firewalls with access control lists, dedicated monitored firewall, and virus and spyware scanning to provide this level of security.

- Policy management – centralized policy management tools are essential to the maintenance of a secure network. Bay Aging uses a series of software and

hardware to analyze, interpret, configure, and report on the state of the security systems.

WAN equipment is considered part of the strategic systems for Bay Aging. Standards for the physical security for all WAN equipment physically located at Bay Aging are the same as those for other strategic systems:

- The premises must be physically strong and reasonably free from risk of damage by water, fire, vibration, dust, and environmental hazards.
- Air temperature and humidity must be controlled within acceptable operating limits.
- Backup electrical power, such as that from an uninterruptible power supply (UPS) or generator, must be available to provide the following:
  - A minimum of 30 minutes on base and 60 minutes of operation on battery packs in the event of a power failure.
  - Adequate protection from power surges and sags.
  - "Power Shute" triggers an orderly shutdown of affected systems 10 minutes before the UPS batteries are depleted.

The primary location for most of the WAN equipment at Bay Aging is at the Agency's Data Center located at Data Center located at 5306 Old Virginia Street, Urbanna, Virginia.

WAN equipment located at Bay Aging is located in a specifically designated secure area. Access to this area is restricted to only authorized personnel from the IT Department and the Agency's Computer Consulting Firm. All other access by other individuals, whether employees or not, must be granted by an authorized member of the personnel and documented on the Server Room Visitor's Log. External doors to the designated area must remain locked. External windows must be secured so as not to allow unauthorized access.

The designated area(s) for the location of WAN equipment must be protected by fire detection and suppression equipment. Fire suppression equipment should be of such a nature that it would not harm computer equipment. Fire extinguishers are available in the event of a small fire that can be easily handled by an individual.

External Access via Virtual Private Network (VPN)

Access to certain Bay Aging systems is available for authorized users through the Internet via the Agency's secure Virtual Private Network (VPN) connection. Other than this VPN connection, Bay Aging does not allow or support the use of external modem access to its internal systems. However, the Agency recognizes that some vendors and third-party providers may require such access for the ongoing maintenance of systems. In such specialized cases, direct, external modem access is allowed, provided the following proper security measures are taken:

- Management Information Systems Director or a member of the Agency's senior management must authorize the remote access.

- Remote access is only allowed during normal business hours.

- Remote access is only provided through the use of a licensed copy of software that allows such access to occur.

- When a vendor is approved for remote access, Network Support Specialist must confirm the *remote* product has been installed on a vendor's computer. The host product is then loaded on the appropriate computer at the Agency.

- The software product is to be configured with the highest available level of data encryption.

- Passwords must be assigned to allow the vendor to attach from the remote to the host.

- If a "call back" feature is available, it must be used. The vendor will initiate a session from the remote to the host. The host will then disconnect from the remote and call the remote. If all logins proceed successfully, access is allowed.

- The vendor will be limited to the minimum amount of security required to perform the necessary duties while the session is active.

- IT Department must monitor the activity performed by the vendor on Bay Aging's systems as closely as possible.

- The remote session must be terminated as soon as the vendor has finished his or her work and the modem powered off.

- The host session must be disabled immediately after the session is terminated.

- A Vendor Access Log must be completed for all remote sessions detailing the date, time, purpose of session, vendor representative, and the Agency employee monitoring the session.

Internet

Bay Aging recognizes the convenience, power, and necessity of the usage of the Internet as another tool to help the Agency maintain a competitive advantage. However, the advantages the Internet brings to the Agency must be tempered somewhat by the additional security risks associated with its use.

Internet Service Provider

Bay Aging currently has contractual relationships with MetroCast Cable and Verizon as its primary and secondary Internet Service Providers (ISPs). As a result of this outsourced relationship and the nature of the Internet, the management of Bay Aging recognizes that it has no control over data traffic that occurs over the Internet. The Agency recognizes the challenge inherent in protecting itself against compromising systems security because of this Internet connectivity. In recognition of this fact, Bay

Aging has taken steps to ensure that the integrity of the data that moves through its Internet connection is not compromised. Four key elements of security are employed:

- User identification – each user of a system must be accurately and positively identified. Bay Aging uses password authentication on all of its systems for this purpose.

- Perimeter security – this element of security ensures that only authorized traffic passes through the network. Bay Aging uses routers with access control lists, dedicated monitored firewall, and virus and spyware scanning to provide this level of security.

- Data privacy – network communications must be kept confidential and protected from eavesdropping. Bay Aging uses generic routing encapsulation (GRE) and digital encryption to protect the privacy of the data moving through its networks.

- Policy management – centralized policy management tools are essential to the maintenance of a secure network. Bay Aging uses a series of software and hardware to analyze, interpret, configure, and report on the state of the security systems.

To some degree, Bay Aging's Internet access can be seen as an extension of its overall Wide Area Network.

Electronic Mail

Bay Aging makes extensive use of electronic mail (email) in its business practices. The need to monitor email messages for dangerous, offensive, or confidential content has never been more evident. The most deadly viruses, those able to cripple an email system and corporate network in minutes, are being distributed worldwide via email in a matter of hours (for example, the "Love Letter" virus). Anti-virus vendors cannot update their signatures in time to protect against all viruses. Worse still, email is likely to become the means for installing "backdoor" and other harmful programs to help potential intruders break into a network.

To safeguard the mail server and network from these types of invasions, Bay Aging utilizes a third party enterprise email security solution provided by Postini, a global leader in Integrated Message Management. The use of their services assists us with the elimination of spam, and supplements and improves our anti-virus protection by providing it at the gateway level thus keeping these threats from ever reaching our network.

Bay Aging uses a comprehensive email security and content checking product to safeguard the mail server and network from those types of invasions.

End users are also instructed through the Bay Aging *Electronic Communications Policy* in the proper handling of email.

Web Browser Software

In order to provide stability and to help the IT Department in deploying browser software, Bay Aging has adopted Microsoft's Internet Explorer browser software with 128-bit

encryption as the corporate standard. 128-bit encryption is the highest level of encryption currently available in browser software.

Internet Monitoring Software

Bay Aging recognizes the need for Internet usage monitoring, not only from a productivity standpoint, but also from a legal standpoint. Bay Aging acknowledges three particular areas where Internet usage abuses could result in legal problems:

- Sexual harassment – this can be the result of bringing objectionable material into the workplace. Although this legal territory is still somewhat uncharted, if an employee downloads objectionable materials – pornography, for example – and another employee sees it, the Agency could be liable. Even worse, if a user downloads materials that violate local, state, or federal laws, the Agency might even face criminal charges.

- Copyright infringement – software programs, photographs, or proprietary documents that can be downloaded by employees from the Internet may be copyrighted.

- Misrepresentation – this can occur particularly through the use of email. Employees should know, and should make it clear to the people with whom they communicate, that opinions expressed via email and other electronic media are their own, not the company's.

Internet File Transfers

Bay Aging recognizes that Internet file transfers will occasionally be necessary as part of its business practices. It also recognizes the danger inherent in allowing files to be exchanged with other entities outside the Agency. As a result, Bay Aging prohibits the transfer of files between its systems and any other entity without the consent of a member of the Agency's senior management. Downloading files from a trusted site can be performed provided the conditions described above are met. Any files downloaded must be screened with virus detection software prior to being invoked. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

Uploading data to any Internet source is subject to stricter standards. Files or data containing customer information should never be transmitted to another source unless the following conditions (in addition to the restrictions listed above) are met:

- Data containing confidential information must be encrypted
- The recipient must be providing some service to Bay Aging
- All laws and regulations regarding customer privacy must be met.

STANDARDS AND GUIDELINES FOR DESKTOP SYSTEMS

Bay Aging has prepared and adopted a separate Microcomputer/Network Policy. It should be referred to for restrictions and guidelines concerning microcomputer use. However, following are some broad guidelines for use of desktop computer systems within the framework of Information Systems Security.

Desktop computers are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units. Desktop computers include personal computers (PC's). Users of desktop computers are subject to the restrictions and guidelines for use specified in the Bay Aging Microcomputer/Network Policy.

In addition to or in conjunction with the restriction and guidelines provided by the Microcomputer Policy, the following guidelines should be considered.

Hardware Security

Desktop systems are to be physically secured to the extent possible. Office keys are registered and monitored to ensure they are returned in the event the employee resigns or is terminated.

It is the responsibility of every employee of Bay Aging to monitor desktop systems, which are located in open areas where the public has access, for unauthorized usage.

All removable media, such as floppy disks, removable hard disks, zip disks, and CD-ROM media is to be stored in a secure location when a desk is left unattended.

The IT Department is responsible for maintaining an inventory of computer equipment to ensure that all equipment is properly maintained, accounted for and to facilitate compliance with any leases, agreements, or service plans.

The IT Department is also responsible for maintaining an inventory of software currently in use by the Agency. The purpose of the inventory is to facilitate compliance with license agreements, monitor vulnerability and patch release information, and to promote efficient operations.

The IT Department is responsible for proper removal and disposal of obsolete computer equipment. This process mandates the removal and destruction of the computer hard drive.

All computers are located away from environmental hazards.

Critical data backup media is sent to the Agency's offsite storage facility.

A current inventory list of all desktop systems is maintained by the IT Department.

Access Security

Password protection is used to ensure that only authorized users can access a system. If the desktop is located in an open space or is otherwise difficult to physically secure,

then automatic screen saver passwords and BIOS passwords should be used. Password guidelines are addressed previously under Password Controls.

Data and Software Availability

Important files and programs must be backed up on a regular schedule. Data and software integrity should be checked and verified on a regular basis. Software problems should be reported to the IT Department immediately.

To ensure that information is properly backed-up and stored, users are directed to save all files and other work to the designated network directory. As the network is a shared resource and storage space is limited, users are directed to manage their saved information within reasonable limits.

Confidential Information

Data transmitted via the Internet must be encrypted. Reports should be removed from printers immediately to prevent unauthorized persons from viewing sensitive data. Fixed disks, floppy disks, or cartridges no longer used must be destroyed in such a manner to prevent recovery of the data contained therein.

Software

Copyright laws protect software, and unauthorized copying is a violation of these copyright laws. Anyone who uses software must understand and comply with the license requirements of the software. Bay Aging is subject to random license audits by software vendors from whom it has purchased software packages.

Viruses

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.

To decrease the risk of viruses and limit their spread:

- Check all software before installing it with the Agency's virus detection software.
- Use the virus detection software to detect and remove viruses.
- Isolate immediately any contaminated system.
- Report immediately any contaminated system to the IT Department.

Computer Networks

Networked computers require more stringent security than stand-alone computers because they are access points to computer networks. While the IT Department is responsible for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating his or her own computer with ethical regard for others in the shared environment.

The following considerations and procedures must be followed when using the Bay Aging network:

- Check all files downloaded from the Internet. Avoid downloading shareware files.
- Test all software before it is installed to make sure it doesn't contain a virus/worm that could have serious consequences for other personal computers and servers on the Agency's networks.
- Choose passwords with great care to prevent unauthorized use of files on networks or other personal computers.
- Always save working files to the Network server where back-ups are performed nightly.
- Never store passwords or any other confidential data or information on a laptop or home PC or associated floppy disks or CDs. All such information should be secured after any dial-up connection to the Agency's network.

Standards and Guidelines for Oversight

In order to ensure enforcement and adherence to the standards and guidelines established within this policy, Bay Aging's senior management as well as the Management Information Systems Director and management-level representatives from each functional area of the Agency has the responsibility to see that this policy is adhered to.

IT Management has the following specific responsibilities:

- Keep the Information Systems Security Policy and procedures current.
- Review purchases of computer hardware and software.
- Review/approve all movement of sensitive data between computers.
- Review all projects that result in man-hours being spent on the programming of computer software.
- Ensure software and hardware licenses are maintained.
- Monitor the installation of software updates and releases.
- Review reports on Disaster Recovery testing and ensure the occurrence of the tests on a periodic basis.
- Ensure that external audit(s) of the microcomputer network or networks occur annually.
- Review error and problem summaries to determine and correct repetitious problems.

IT Department

The IT Department has the primary responsibility for day-to-day oversight of Information Systems. The Information Systems oversight duties of the IT Department include:

- Monitoring operations of all computers and software.
- Adding approved new users to systems.
- Troubleshooting systems problems.
- Maintaining current inventories of the software and hardware components that make up Information Systems.
- Capacity monitoring and planning for all systems.
- Acquiring and deploying systems.
- Installing new software and upgrading existing software.
- Managing outsourced vendor relationships.
- Cooperating fully with regulatory and auditing agencies.

Users

All users are responsible for adhering to the Agency's policies and maintaining an ongoing awareness of appropriate computer usage and security practices.

GLOSSARY OF TERMS

Confidential:	Containing personal or sensitive information that is not to be shared with unauthorized persons.
Data:	Numerical or other information represented in a form suitable for processing by a computer.
End-user:	An individual who uses a microcomputer.
Hardware:	A computer and the associated physical equipment directly involved in the performance of data processing or communications functions.
Microcomputer:	A very small computer, such as a laptop or personal computer, built around a microprocessor and designed to be used by one person at a time.
Microprocessor:	An integrated circuit that contains the entire central processing unit of a computer on a single chip.
Network:	A system of computers interconnected by telephone wires or other means in order to share information.
Proprietary:	Made and sold by an individual or firm having exclusive rights of manufacture and sale.
Security:	The state of being free from acceptable risk.
Software:	The programs, routines, and symbolic languages that control the functioning of computer hardware and direct its operations.
Spyware	Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that

	information in the background to someone else.
Strategic Systems:	Computer systems that are critical to the operation of an organization.
Unauthorized:	Unsanctioned, unlawful, not justified.
Uninterruptible Power Supply or UPS:	A device containing rechargeable batteries capable of allowing computer systems to operate for temporary periods during utility power interruptions.
Virus:	Malicious, self-propagating computer programs that are sometimes attached to computer files or other programs and can be used to damage computer systems.