INFORMATION SECURITY POLICY

I. PURPOSE

This directive provides the policy and procedures for safeguarding electronic information and systems throughout the Village of Estero (Village). The purpose is to protect the rights of citizens and employees and to fully comply with Village policies and with State and Federal laws. This directive defines the requirements needed to mitigate the security risk(s) created by unauthorized access, loss, release, destruction, or modification, of Village Electronic Information.

DEFINITIONS

A. **Access** - To log into, instruct, communicate with, store in, retrieve from, or otherwise use a computer or Village electronic information.

B. **Village Manager, IT Department, and Department Director** - Those persons and any designee(s) of those persons.

C. **Computer** - Electronic devices that can store or process information or data by manipulating magnetic, optical or other inputs in order to acquire, create, access, modify, store, manipulate, manage, move, control, display, switch, interchange, transmit, process, receive, or produce data or information. The term includes individual devices whether or not connected to the Village Network, and accessories including output, processing, storage, media, memory sticks and other storage devices, memory, software, communications, and other ancillary devices and equipment. A Village computer is any computer owned by the Village.

D. **Village Electronic Information** - Any and all information, data, software, security measures, e-mail, or other material that is acquired, created, accessed, modified, stored, manipulated, managed, moved, controlled, displayed, switched, interchanged, transmitted, processed, received or produced electronically.

E. **E-Mail** - Any system used by the Village of Estero that allows the electronic communication of messages via computer between a sender and one or more recipients, and any message(s) produced through the system. The term “message” includes any attachment(s) to the message.

F. **Firewall** - A computing platform or electronic device that serves as a barrier to protect other computing platforms on the network from being directly accessed.

G. **Network** - A configuration of computers, devices and software connected for information exchange.

H. **Password** - A string of characters used to gain access to Village electronic information.

I. **Publicly Accessible Electronic Information** - Village electronic information that the general public may access on a read only basis.

J. **Security Measures** - Codes, passwords, encryption methodology, hardware, software or other equipment, policies, or procedures that restrict access to a computer or Village electronic information, secure the computer or Village electronic information from destruction or modification, or otherwise assure the availability, confidentiality, security and integrity of the computer or Village electronic information.

K. **Software** - Includes, but is not limited to, source and object programs, shareware, netware, utilities, diagnostic programs, operating systems and communication programs.

L. **User** - Any person or entity who accesses Village electronic information.

II. POLICY

As further described in this directive, Village electronic information:

- Is the sole property of the Village, and users have no personal or property rights to the information.
- Shall be protected to ensure the information is available when needed, and is secured from unauthorized access, modification, or release.
- Shall only be released or made accessible to the public by department director approval, in accordance with the Florida Public Records Statutes and other applicable laws, and Village or department policies.
- Shall, except in the case of publicly accessible electronic information, be accessible to persons other than Village employees only with proper authorization.

III. GENERAL

A. Village Ownership of, and Right of Access to, Village Electronic Information

Village electronic information is solely the property of the Village, regardless of physical location or how maintained; users have no personal property, privacy or other rights in it.

As owner, the Village has, at all times, the right of access to Village electronic information whether or not it has been made subject to security measures. The Village Manager may access Village electronic information within any department or office, and department directors may access Village electronic information within

their respective departments. Where necessary, assistance in obtaining authorized access shall be provided by the IT Department. Any user shall cooperate in the access of specific Village electronic information at any time upon an authorized request.

The accessing of a department's Village electronic information shall be coordinated with the department director unless the Village Manager determines that the access should remain confidential.

B. Security of Village Electronic Information

Village electronic information, including publicly accessible electronic information as appropriate, shall be secured from unauthorized access, destruction or modification. Access shall be in compliance with any applicable legal requirements and Village and department policies and procedures.

Software and hardware security products selected as standards will be used for all computer systems and equipment that contain restricted information. These products will provide for ease of access while still securing the information. Non-standard security products may be authorized by the IT Department on a case by case basis upon justification by the department requesting the exception.

C. Release of Village Electronic Information to the Public

Release of Village electronic information to the public, including both release in response to public records requests and the categorization of Village electronic information as publicly accessible electronic information, shall be by department director approval, in accordance with the provisions of the Florida Public Records Statutes and Village or department policies. Any questions concerning release of Village electronic information should be directed to the Village Attorney's office. The Village will determine the form in which Village electronic information is to be released, unless the form is specified by law.

Nothing in this directive shall be construed as a statement or admission by the Village that any particular Village electronic information is in fact subject to disclosure under the Florida Public Records Statutes. Such a determination will be made on a case by case basis.

D. Access by Non-Employees to Village Electronic Information

Non-employees may not access Village electronic information, beyond that which the Village has made publicly accessible, unless authorization is obtained from the Village as provided below:

1. A department director may authorize persons who are providing services to the department (e.g., consultants or employees of temporary agencies) to access information from a Village computer, if such access is necessary to carry out

their work assignments on behalf of the Village, and consistent with the Village's policies and security requirements.

2. A department director may, on a case by case basis and in consultation with the Village Attorney's office and the IT Department, authorize other users, including contractors and governmental agencies, to access Village electronic information from a Village or a non-Village computer, if such access is necessary to carry out the user's work assignments, deemed beneficial to the Village, and consistent with the Village's policies and security requirements. The user must demonstrate to the Village's satisfaction that the Village electronic information will remain confidential and will be protected by adequate security measures.

E. Distribution of Directive and Compliance with Requirements

Departments shall make available a copy of this directive to all computer users. Users shall comply with the provisions of this directive and shall be subject to penalties for failure to comply with any requirement.

In addition to civil or criminal remedies or sanctions available to the Village under law, penalties for violation of this directive may include:

For Village employees - appropriate disciplinary action, up to and including termination.

For non-employees - immediate loss of the privilege to use any Village computer and Village electronic information, and other sanctions available to the Village, such as contract revocation.

IV. RESPONSIBILITIES

A. IT Department Responsibilities

Security issues posed by the implementation of networks are Village-wide in scope, since breaches of security on networked devices may present risks to other resources on the network. Inter-network connections to other agencies, the Internet and remote access can present serious threats to the security of the entire network. The IT Department is responsible for maintaining security at the Village network level, and shall provide oversight, design and administration for resources which impact network security.

B. Departmental Responsibilities

Since departments are most familiar with their information processing, they are best qualified to identify their Village electronic information and indicate how and to what extent it should be secured, based upon legal considerations or departmental policies, and assistance, upon request, from the IT Department.

1. Each department shall secure its Village electronic information from unauthorized access, destruction, or modification; prevent unauthorized access to its computers; dispose of unnecessary information; monitor user compliance with security procedures; and restrict access to confidential information (e.g., computerized employee information) to those users whose duties require access.

2. To ensure that the Village's computers and electronic information are not subject to modification by former users who should no longer have access:

    - The Department of Human Resources shall inform the IT Department of all employee resignations and terminations.

    - Each department shall notify the IT Department when any contract personnel or consultants, who have been authorized access to computer systems managed by Information Technology, have completed their service to the Village.

    - Should a department desire to temporarily limit an employee's access (e.g., when the employee is on an extended leave of absence or suspension), the IT Department shall also be notified.

C. <u>User Responsibilities</u>

1. Users shall assist in maintaining the security of Village electronic information through the steps set forth in this directive.

2. Except where designated as publicly accessible, Village electronic information shall be accessed only for official Village business and purposes, and for such other activities as may be necessary and desirable to meet Village organizational needs and goals. Access for other purposes is prohibited.

3. Village employees, and non-employee users authorized to access Village electronic information pursuant to Section IV.D, shall not access or attempt to access Village electronic information except where necessary to the performance of their work assignments. This section shall not be construed to prohibit the use of training or tutorial software or similar activities that may improve users' ability to carry out their work assignments.

4. Persons using publicly accessible electronic information shall not attempt to circumvent security measures relating to such information, nor take other action that might compromise the availability, security or integrity of that information.

5. A user's personally owned software or hardware shall not be installed on any Village computer or network except as provided under Section VI.C.

6. Users shall not attempt to obtain information regarding any security measure(s)

for computers or Village electronic information to which they do not have authorized access.

7. Except as may be necessary to permit access by authorized Village personnel, users shall not share information regarding the security measures that protect computers or Village electronic information relating to their work assignment without the prior consent of the director of the department providing access to the user.

V. SECURITY MEASURES

A. Normal security measures for Village electronic information include locked desks, filing cabinets, and offices; password access to resources beyond the desktop workstation; file backups; effective scanning for viruses; establishment of standards, rules and procedures for access to systems; and assurance that the appropriate personnel deal with systems.

Further security measures may be necessary as the availability, integrity, or confidentiality of automated system data becomes more important to regular operations.

B. Virus protection shall be utilized on all Village computers. When a virus is detected, the user shall immediately notify the IT Department.

Since viruses can easily spread, removal shall be coordinated through the IT Department in order to guarantee complete removal of the virus from Village computers. The IT Department has responsibility for the final determination of appropriate virus removal measures.

C. Mission critical files shall be backed up in accordance with established department guidelines, and the backup secured in a location sufficiently separate from the primary storage device to provide for the recovery of lost or damaged files.

D. To the extent possible, publicly accessible electronic information will not be encumbered by onerous access controls. However, firewall systems will be implemented to separate it from other Village electronic information requiring a greater level of control.

E. Access to Village electronic information by authorized employees or non-employee users shall occur through access keys, passwords and other suitable security measures. Security measures, including virus protection, will be regularly reviewed and changed as often as deemed necessary by the department to protect the security of its Village electronic information.

F. All connections to non-Village networks will be secured by firewalls designed to permit users with specific needs to access only those resources necessary.

VI. User Access Reviews

A. The Village shall review all active accounts for users who can access Village data, and ensure that their ability to access and level of access is appropriate. This review shall be conducted on an annual basis at the beginning of the Village's fiscal year, and should be conducted by the IT Department in communication with all other Village Departments to review current active users.

The review should follow the below methodology:

1. Produce a record of all Active Directory system user accounts, including specific levels of access (if applicable)
2. Produce a record of all financial system user accounts, including specific levels of access (if applicable)
3. Review the user accounts to determine if they are still active and if their level of access is appropriate
4. Remove users who are no longer active and adjust levels of access if necessary
5. Provide a formal report to the IT Manager and Department Heads for review and signed acceptance
6. Produce a formal document outlining all user access review activities performed for audit documentation purposes including but not limited to:
    a. Names and positions of authorized employees/contractors who conducted the reviews
    b. Date the reviews were performed
    c. Access changes that were completed