Summary of the Pinellas County Information Security Policy

All computer users (employees and third parties such as contractors) must adhere to the Pinellas County Information Security Policy. This policy is found on the County's Intranet (Intraweb). All users are expected to comply with this Policy as a condition of continued employment, so it is important that you read and familiarize yourself with the policy.

The purpose of this Information Security Policy is to:

- Protect information technology.
- Minimize liability and determine acceptable risk related to information and information technology.
- Assign responsibility and roles for information and information technology.

The following is a summary of the highlights of the policy.

Passwords/Passphrases:

- Passwords/Passphrases are your "keys" to the Pinellas County Network. Users must maintain control of their personal passwords and must not share them with others,
- Your password/passphrase must have a minimum of 14 characters and contain letters, numbers and, if the system permits, symbols.
- Your password should not be found in any dictionary (English or foreign) or contain common character sequences (such as 12345678).

Computer Use and the Permissible Use of Information:

- Information and Information Systems must be used for business purposes only unless expressly authorized by management.
- Users must not read, modify, delete, or copy a file belonging to another user without first obtaining permission from the owner or someone else authorized to grant such permission.
- Unless general user access is clearly provided, you may not read, modify, delete, or copy a file belonging to another user.
- Browsing through computer systems or networks is prohibited. You may not search for interesting files or programs in the directories of other users. A legitimate attempt to locate information needed to perform one's job is allowed, as it is not considered browsing.
- Access to the Pinellas County internal network from remote locations such as homes, hotel rooms, and customers' offices, must be approved in advance by the user's immediate manager and the Information Security Section must be notified prior to that access.

Software and Hardware Use:

- You may not install any software on computers unless you obtain prior approval from management.
- Users must not change operating system configurations, upgrade existing operating systems, or install new operating systems on any devices without obtaining advance permission from their Agency management.
- Users may not disable virus detection programs.
- Users may not install any hardware on County computers without obtaining advance permission from management.

- Programmers and other technically oriented staff must not install back doors that circumvent the authorized access control mechanisms.

Reporting of Security Breaches:
Any issues related to security breaches such as viruses and unauthorized access should be reported to your systems administrator immediately. The systems administrator should contact both the BTS Operations Center at 727-453-HELP (4357), and the IT Information Security Officer.

Email:
- The Internet should be used for government purposes only.
- All incoming emails must be scanned by antivirus software.
- Messages and/or attachments found to pose a threat will be quarantined or deleted.
- The sending of unsolicited commercial email ("Spam") is prohibited.
- All mail sent to and from Pinellas County Government is subject to the Public Records Law of Florida.

Public Records:
- Most records produced in the course of government business are public and open to inspection by anyone who asks. The Information Owner (generally elected officials) may regulate the time and manner of such inspections.
- The fact that information is public record does not mean that it may be disclosed in any manner that the employee or contractor sees fit; some information such as information protected under the HIPAA guidelines and Security Information (passwords, user accounts, and other security information) are exempt.

Information Users Responsibilities:
- Information users are individuals who have been granted explicit authorization to access, modify, delete and use information by the owner. You are an information user if you have access to a computer.
- Users must protect the information to which they have been granted access.
- Users must report to the owner any information security vulnerability or violation.

This is just a summary of the Information Security Policy. All information users are responsible for becoming familiar with the rules found in the policy. You may access the complete Pinellas County Information Security Policy (internal link).

Acknowledgment
As a condition of employment, I have read, understood, and will adhere to the above guidelines for access and use of information found in the Pinellas County Information Security Policy.

Signature: _____

Name: _____

Department: _____

Date:_____

Employee Number: _____(FOR USE BY HR)