Fairfield County Government
Data Breach Incidence Response Policy

1.0 Purpose

To prevent tarnishing the public image of Fairfield County Government and prevent the unwanted loss of data

2.0 Scope

This policy covers appropriate actions to take in case of a virus or other incident that could allow the loss of data or corruption of data. It also covers preventive measures that may avert incidences; averting is optimal to reacting

3.0 Relevant Definitions

Spyware- Software that self-installs on a computer, enabling information to be gathered covertly, about a person's Internet use, passwords, etc. However, it's usually delivered to a computer by some inadvertent action of the end-user

Malware - Software that is intended to damage or disable computers and computer systems

Virus - A computer virus is a computer program that can replicate itself and spread from one computer to another via some human action such as email sharing or file sharing

Trojan Horse- a.k.a.- Trojan, is a non-self-replicating type of malware which appears to perform a desirable function but instead facilitates unauthorized access to the user's computer system. Trojans do not attempt to inject themselves into other files as a computer virus will. Trojan horses may steal information, or harm their host computer systems. They generally masquerade as a wanted program but after downloaded will execute some non-related action designed by its creator

Marvin L. Allen
I.T. Director

5/15/2013

Encryption . The translation of data into a secret code.

AV . Anti-Virus Software

Mission Critical . Any system that is necessary for the function of Fairfield County government, including but not necessarily limited to Finance, Payroll, Tax Collection/Treasurer, E911, Sheriff, Jail

4.0 Prevention. Fairfield County IT recommends that users change their passwords to computers and sensitive information often and use passwords that are at least 8 characters in length with a mix of upper and lower case and include numbers. We enforce a 15 day password change for our Finance Package (Logos.NET), for example. We configure each computer with a user account password and demonstrate how to lock the system if the user is not familiar with PC operations

We provide a core network firewall (Cisco ASA) with advanced features to thwart invasions and risks of invasions. Furthermore, each local PC has a firewall that we install along with the AV program

We install anti-virus software on each computer and configure it for daily updates and weekly scans. Furthermore, we configure the AV program for aggressive real-time scanning and monitoring that will either delete or quarantine any suspicious activity.

We provide, configure and monitor backup software for all mission critical systems and we provide, configure and instruct non-mission critical system users on backup procedures that they may feel are relevant to their department

We provide and recommend encryption software for anyone with sensitive files stored on their computers and removal backup media

We do not condone or knowingly allow personal devices to be used in our network (i.e. iPads, iPhone and laptops from home). We configure our switches with port security to not allow more than 2 devices for *most* ports (PC and phone) and we change WiFi passwords periodically in case someone has been able to supersede the WiFi security

5.0 Reaction

If a breach of security occurs (virus found on a PC or any other suspicious PC activity) we have informed (and it's common knowledge) users to report such incidences to the IT Department right away. At such time, Fairfield County IT will react by first investigating the PC in question to observe PC behavior. If we determine that a virus or spyware has infiltrated the system, we will ask pertinent questions to determine why/how it occurred.

We may then use that investigative knowledge to amend the core firewall rules and/or local AV and firewall to stop further infiltration. We then take action to remove the unwanted program (virus, spyware, malware, etc.) from the PC. The removal action is commensurate upon the severity of the case at hand and can range from a simple system restore to a full ablation of the hard drive,

5.1 Monitoring

We will monitor the system that was infected for a few days after taking the appropriate action from step 5.0 to determine if our remedy was successful. If successful, we close the case, otherwise we take more aggressive action to find remedy

5.2 Enforcement

Enforcement of this policy is done to the best of the Fairfield County IT Department's ability in relation to cooperation from each department manager. We do not/cannot set disciplinary action for other departments, but we can and will prevent the distribution or use of a computing device in an area that may violate the letter and/or spirit of this policy

6.0 Encryption

All removable media (thumbdrives, CDs/ DVDs etc.) with sensitive data should be encrypted with a password set by the user in agreement with that employee’s department manager. IT will provide cryptographic software and instruct authorized users on procedures and best practices.

Policy Approvals

Prepared by Marvin L. Allen
Information Technology Department Director

Date June 13, 2013

Ammended April 27, 2015 for section 6.0 ____________________

Davis Anderson
Deputy Administrator

Approved by ______________________________
Administrator

Date ____________________ 6-13-2013