FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: Computer Malware Protection Procedures

Related Policy: FDJJ – 1205.20

I. DEFINITIONS

Compromised Computer – A computer that has been infected by malware, which can be used to attack other computers connected to a network. It may also lead to malicious exposure of the data stored on the computer.

Internal Network – Any network subject to a firewall.

Malware – Any type of malicious software (malware) designed to damage or steal information and/or act in an unexpected or undesirable manner. Malware includes but is not limited to rootkits, spyware, Trojan horses, and viruses. Also referred to as malicious code.

Mobile Computing/Storage Devices – General term used to describe both mobile computing and mobile storage devices and/or media including, but not limited to, external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), iPods, media players, and mobile phones or tape drives that may be easily attached to and detached from computing devices.

Ransomware – A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

Users – Florida Department of Juvenile Justice (DJJ) employees, employees of providers, contractors, vendors and third party organizations using or accessing DJJ-owned computers or connecting to DJJ's internal network.

II. STANDARDS/PROCEDURES

A. Implementation of Malware Detection/Prevention Program:

1. Each personal computer shall be virus checked prior to installation with the standard malware detection software approved by the DJJ Bureau of Information Technology (IT).

2. IT shall be responsible for installing and upgrading malware detection/protection software on every computer and server within the DJJ system.

3. The malware detection/protection software will be routinely inspected for compromised computers and servers.

4. IT shall utilize technology and tools to protect the DJJ network from known vulnerabilities; including, but not limited to, installing operating system patches and updates, blocking

potentially malicious websites, email messages from known spammers and certain email attachment types.

5. All mobile computing/storage devices from outside sources used on Department owned computers shall be scanned and verified with the Department's malware detection/protection software prior to opening files on said device.

B. Compliance with the Malware Detection/Prevention Program:

1. DJJ staff, providers, contractors, vendors and third parties using or accessing Department-owned computers or connecting to the Department's internal network shall not disable, bypass, or alter in a manner that will reduce the effectiveness of the Department's malware detection/protection software.

2. Users of Department-owned computers or connecting to the Department's internal network shall immediately notify the Bureau of Information Technology if he/she suspects their computer has been compromised (see next section, Section C. for examples)

C. Possible Compromised Computers:

1. Listed below are indicators or signs that may suggest a computer has been compromised:
   a. Programs pop up unexpectedly or other unexpected behavior;
   b. Unusually slow or non-responsive;
   c. Show signs of high hard drive activity, not based on your commands or activity;
   d. Displays messages you have not seen before;
   e. Runs out of disk space unexpectedly;
   f. Unable to run a program due to lack of memory- and this has not happened before;
   g. Constantly crashes;
   h. Rejects valid/correctly entered passwords; or
   i. Files that have been renamed and encrypted along with a message demanding payment in exchange for unencrypting the files. (e.g. Ransomware).

D. Penalties for Violation:

1. Violation of any provisions of this policy may result in revocation of access/permissions and is cause for disciplinary action up to and including dismissal, civil fines or tort action, and/or criminal prosecution under Chapter 815, Florida Statutes, or other applicable federal, state or local laws.

III. RESPONSIBILITY AND DUTIES

A. Secretary:

1. Shall support a comprehensive malware detection/prevention program.

B. Chief, Information Technology:

1. Shall develop, coordinate, implement, and maintain procedures and guidelines.

C. Information Security Manager:

1. Implement the policy stated in this directive.

2. Shall ensure the proper governing agency is notified of malware compromises, which cause large-scale, network-wide outages, and/or threats, which cause or have the potential to cause significant outages to multiple organizations.

3. Shall work with the Department's network administrator to:

   a. Administer an anti-malware program; and

   b. Monitor and/or audit computers for malware.

D. User:

1. Responsible for complying with this policy and procedures and observing the agency's policies and procedures identified in the "Related References" section of this policy.

2. Shall not disable, bypass, or alter in a manner that will reduce the effectiveness the Department's malware detection/protection software.

IV. ATTACHMENTS N/A