Removable Media

1.0 Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

2.0 Purpose

To minimize the risk of loss or exposure of sensitive information maintained by <Company Name> and to reduce the risk of acquiring malware infections on computers operated by <Company Name>.

3.0 Scope

This policy covers all computers and servers operating in <company name>.

4.0 Policy

<Company Name> staff may only use <Company Name> removable media in their work computers. <Company Name>removable media may not be connected to or used in computers that are not owned or leased by the <Company Name> without explicit permission of the <Company Name> info sec staff. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the <Company Name> Acceptable Encryption Policy:
http://www.sans.org/resources/policies/Acceptable_Encryption_Policy.pdf
Exceptions to this policy may be requested on a case-by-case basis by <Company Name>-exception procedures.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including
termination of employment.

6.0 Definitions

Removable Media: Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without

modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by <Company Name>.

Encryption: A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

Sensitive Information: Information which, if made available to unauthorized persons, may adversely affect <Company Name>, its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers and , financial information,

Malware: Software of malicious intent/impact such as viruses, worms, and Spyware.

7.0 Revision History

Original Issue Date: