Software Installation Policy

1.0 Overview

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered in an audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment.

2.0 Purpose

To minimize the risk of loss of program functionality, the exposure of sensitive information contained within <Company Name's> computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

3.0 Scope

This policy covers all computers, servers, PDAs, smartphones, and other computing devices operating within <Company Name>.

4.0 Policy

Employees may not install software on <Company Name's> computing devices operated within the <Company Name> network. Software requests must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk in writing or via email. Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

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

DLL: Dynamically Linked Library. A shared program module used by one or more programs, often installed as part of a program installation. If the current version of a DLL is overwritten by a newer or older version, existing programs that relied upon the original version may cease to function or may not function reliably.

Malware: A wide variety of programs created with the explicit intention of performing malicious acts on systems they run on, such as stealing information, hijacking functionality, and attacking other systems.

PDA: Personal Digital Assistant. A portable, hand held computing device capable of running software programs. It may connect to host computers or to wired or wireless networks.

Smartphone: A cellular phone with qualities of a computer or PDA. It is capable of running software programs and connecting to computer networks.

7.0

Revision History

Original Issue Date: