Software Installation Policy

Free Use Disclaimer: *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new policy or an updated version of this one.*

1. Overview

Giving employees access to install software on business computers exposes the corporation to undue risk. When employees install software on company equipment, issues like conflicting file versions or DLLs that can prevent programs from running, the introduction of malware from infected installation software, unlicensed software that could be found during an audit, and programs that can be used to hack the organization's network are just a few examples of the issues that can arise.

2. Purpose

A software installation policy outlines the rules and procedures that an **<Company Name>** follows when installing or updating software on its computers and other devices. The purpose of such a policy is to ensure that the software used within the **<Company Name>** is secure, up-to-date, and in compliance with legal and regulatory requirements.

3. Scope

All **<Company Name>** employees, independent contractors, vendors, and agents using a mobile device that belongs to **<Company Name>** are subject to the terms of this policy. This policy applies to all computers, servers, mobile phones, tablet computers, and other computing equipment used by Business **<Company Name>**.

4. Policy

4.1 Employees may not install software on <Company Name's> computing devices operated within the <Company Name> network.

4.2 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.

4.3 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.

4.4 The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

5. Policy Compliance

5.1 Compliance Measurement: The infosec team will use a variety of techniques, including but not limited to business tool reports, internal and external audits, and reporting to the policy owner, to ensure that this policy is being followed.

5.2 Exceptions: The Infosec team must beforehand approve any exception to the policy.

5.3 Non-Compliance: An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies, and Processes

None

7. Revision History

Version	Date	Description
1.0	21-02-2023	Initial Policy