Software Installation Policy

1.0 Purpose

The installation of unauthorized or improperly vetted software on organizational computing devices introduces significant risks. These risks include, but are not limited to, software conflicts leading to system instability or loss of functionality, the introduction of malware (viruses, spyware, ransomware), violations of software licensing agreements leading to legal liability, and the installation of tools that could compromise network security or sensitive data. The purpose of this policy is to establish clear requirements and procedures for requesting, approving, and installing software on all organization-owned computing devices to mitigate these risks.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and any other individuals using computing devices owned or managed by the organization. This includes desktops, laptops, servers, smartphones, tablets, and any other device capable of having software installed that connects to the organization's network or accesses organizational data.

3.0 Policy Statements

3.1 Prohibition of Unauthorized Installation

* Users (employees, contractors, etc.) are strictly prohibited from installing any software onto organization-owned computing devices themselves. This includes downloading software from the internet, installing from removable media (USB drives, CDs/DVDs), or using personal software licenses on organizational assets.

3.2 Software Request and Approval Process

* All requests for new software installation must follow a formal process:
    1. The user requiring the software must obtain written approval (email sufficient) from their direct manager, confirming the business need for the requested software.
    2. Once manager approval is obtained, the user must submit a formal request to the designated IT authority (e.g., Information Technology department or IT Help Desk) via approved channels (e.g., ticketing system, designated email).
    3. The request should clearly state the business justification and the specific software needed.

3.3 Approved Software List

* The designated IT authority (e.g., Information Technology department) will maintain a list of standard, approved software titles that have been vetted for security, compatibility, and licensing compliance.

* Users should first attempt to select software from this approved list if it meets their business requirements.
* Requests for software *not* on the approved list will require additional review and justification regarding the specific need that approved alternatives cannot meet.

3.4 IT Department Responsibilities

* Upon receiving an approved request, the designated IT authority (e.g., Information Technology department) is responsible for:
    * Verifying the business need and approvals.
    * Reviewing non-standard software requests for security risks, compatibility issues, and supportability.
    * Procuring the necessary software licenses through approved channels.
    * Tracking all software licenses to ensure compliance.
    * Testing new software for conflicts and compatibility within the organization's standard operating environment where feasible.
    * Performing the installation of the approved software onto the user's device(s).
    * Maintaining records of installed software.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including software inventory scans, audits of devices, review of help desk requests and software licenses, internal/external audits, and investigation of security incidents potentially related to unauthorized software.

4.2 Exceptions

Any exception to this policy (e.g., granting specific users limited installation rights for development purposes under controlled conditions) requires formal, documented justification, risk assessment, and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

* Unauthorized software found on organizational devices will be removed.
* Users found to have violated this policy by installing unauthorized software may be subject to disciplinary action, up to and including termination of employment or contract. Access privileges may also be restricted.

5.0 Related Policies

* Acceptable Use Policy (AUP)
* Information Security Policy (Overall)
* Change Management Policy
* Procurement Policy

* Workstation Security Policy / Standard

Revision #2
Created 28 August 2024 16:58:37 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery