Software Installation Policy

1. 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 during 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. Purpose

The purpose of this policy is to outline the requirements around installation software on Ilitera computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within Ilitera computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

3. Scope

This policy applies to all Ilitera employees, contractors, vendors and agents with a Ilitera owned mobile devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within Ilitera

4. Policy

- Employees may not install software on Ilitera computing devices operated within the Ilitera 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. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

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 Definitions and Terms
None.

8 Revision History

Date of Change	Responsible	Summary of Change
September 2018	Ilitera Policy Team	Updated and converted to new format.