**Software Installation for Administrators Procedure**

The **[Organization]** grants some of its employees’ local administrative rights on their workstations, in order to allow them to conduct certain business activities more effectively. While this affords more independence, it also opens the organization to increased exposure. Malware can be hidden in legitimate software download packages, unlicensed software can be discovered during an audit and incompatible software can damage an operating system or take down its security features.

# Purpose The purpose of this procedure is to outline the requirements regarding installing software on [Organization] computing devices in order to minimize the risk of:

# Loss of program functionality

# Exposure of sensitive data contained within the [Organization] computing network

# Introducing malware

# Legal exposure of running unlicensed software

# Scope

# All staff, employees, and entities working on behalf of [Organization] are subject to this procedure. This procedure covers all computers, servers, smartphones, tablets, and other computing devices operating within [Organization].

# Procedure

* Only software necessary to the employee’s job function shall be installed.
* It is the employee’s responsibility to ensure that only properly licensed software is installed on **[Organization]** system resources.
* Software should only be installed from trusted sources.
* Software from non-**[Organization]** sources must be scanned for anti-virus and malware.

# Enforcement

Violation of this procedure could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

Under the law, a company can be held liable for its employees’ actions with regard to installing unlicensed software that includes damages of up to $150,000 or more.

1. **Definitions**

* Not applicable at this time