# Standard Software Application Policy

## Overview

A standardized software policy offers better supportability, a more consistent operating experience for users and is one component used to help protect the security of [LEP] resources. [Insert Appropriate Department] is tasked with ensuring that only approved applications are used on computing devices within the organization.

## Purpose

This policy is designed to protect [LEP] by requiring all staff to only run software application programs on deemed safe and standard by the [LEP] [Insert Appropriate Department]. This helps to ensure applications in use by staff meet [LEP] security, functional, and support criteria.

## Scope

This policy applies to all [LEP] staff.

## Policy

The [Insert Appropriate Department] shall prepare and maintain a list of software applications that are approved for general use by staff. Programs that appear on the approved list of software applications shall include general office productivity products (e.g. word processing, spreadsheets, presentations) as well as utility and management programs specific to a department or function (e.g. anti-malware, inventory, help desk, custom applications, on-demand apps and software, etc.).

Only approved software applications are allowed to access [LEP] networks and information resources. Under no circumstances shall staff use programs that are not on the approved list of software applications. Staff members who introduce a security issue by installing and running an unapproved program risk disciplinary action.

Staff are encouraged to use and operate programs that appear on the approved list of software applications wherever possible. However, there are always exceptions based on special use cases. Should a staff member need access to a piece of software that does not appear on the approved list for their work, they must submit a justification request to the [LEP] Helpdesk to evaluate the application and request. This process applies to licensed applications, shareware, freeware, trial programs, and all other software installed on the user’s business computing asset(s). The [LEP] Helpdesk regularly evaluates special requests and also updates the approved list of software applications on an as needed basis.

Special exceptions may be made to this policy for specific employees depending on the required job function and the skills of the employee. Possible reasons for a granted exception include:

* Staff who require specialized software to test new applications on development, test and production networks
* A programmer that must execute non-standard applications in order to test the software
* Network administrators who install and test software as a part of their regular job duties
* Users or contractors providing specialized service functions within the organization

Exceptions are handled on a case-by-case basis by the [Insert Appropriate Role] or their designee and documented.

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP] internal application development and release methodology. Examples of audit based evidence include:

* Samples of the policy implementation in archival documentation
* Regular documented and published updates of approved [LEP] software
* Documentation of approved and disallowed software requests
* Documentation of at least an annual review of software and standards for the [LEP]

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 9/15/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |