# Workstation Security Policy

## Overview

Workstations (either fixed or mobile) are a preferred application access method for many employees located at [LEP] facilities. Information security begins at endpoint devices. This document describes required minimal security configurations for all workstations connected and used in a production capacity on the [LEP] network.

## Purpose

The purpose of this policy is to provide workstation security procedures that ensure information on workstations and the networks they operate on are safe and viable. Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity, and availability of information. This policy helps ensure that access to sensitive information is restricted to authorized users.

## Scope

This policy applies to all [LEP] staff that use, configure, or support desktop workstations.

## Policy

Computer workstation users shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access. The following procedures shall be in force to manage technical, physical, and administrative controls and safeguards for [LEP] workstations:

### PHYSICAL SAFEGUARDS

Physical access to workstations shall be restricted to authorized personnel. Employees shall prevent unauthorized viewing of information on a screen by:

* Ensuring monitors are positioned away from public view
* If necessary, privacy screen filters or other physical barriers to prevent public viewing shall be installed
* Manually activating a password protected screen saver when staff leave their desk
* Exiting running applications and closing any open documents
* Ensuring workstations are logged off at the end of each business day
* Staff shall keep food and drink away from workstations in order to avoid accidental spills

### OPERATIONAL SAFEGUARDS

Employees shall use workstations for authorized business purposes only and only approved personnel may install software on workstations. All sensitive information must be stored on network servers. Staff shall comply with all applicable policies and procedures related to desktop computing.

### MANAGEMENT AND ADMINISTRATION

[LEP] [Insert Appropriate Department] shall ensure that all workstations use a surge protector and/or a UPS battery backup. Workstations shall have all critical security updates and patches installed in a timely manner.

## 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]. Satisfactory examples of evidence and compliance include:

* Spot user checks for compliance with general workstation computing policies
* Documented patch logs for workstations showing patches, dates, and systems installed
* Verification of UPS and/or surge protection installed on physical equipment

## 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 | 11/01/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |