1. **PURPOSE**

The purpose of this Software request /authorization SOP is to provide MIS personnel, faculty, and staff steps to follow when planning to purchase, renew, and install authorized software on FTCC systems.

1. **SCOPE**

This SOP applies to all software assets.

1. **RESPONSIBILITIES**

It is the responsibility of all faculty and staff to follow the procedures and guidelines outlined in this SOP. Exceptions to the above must be reviewed by the Chief Information Security Officer (CISO) with final approval from the MIS AVP/CIO

1. **PROCEDURES**
2. Faculty and staff members shall submit a ticket to the Helpdesk for a Software Request/ Authorization with the following information included**:**

**•** Software name

• Version

• Website

• Link to documentation/source code if open-source

• Business Justification

• EULA

* HECVAT (Required if the software is cloud-based)
* ADA Compliance
1. Before purchasing, acquiring, and downloading software on FTCC systems, the below teams must conduct a risk and security assessment:

**MIS Third-party Management Team**

FTCC third-party management team will do a preliminary review of the software before forwarding the request to the below teams for security vetting;

**Networking**

The Network team to look at the software to ensure it will integrate into the environment without breaking anything and to ensure the software versions are still supported by the vendor.

**The Legal Team Checks**

The legal team to review the licensing agreement/Terms and Conditions;

**Cyber Risk Check**

The Cyber Security team to evaluate the software for any security vulnerabilities/ Privacy policy concerns and make recommendations

1. The CISO shall then decide whether to recommend approval or not recommend approval of the software. The CISO will then send their recommendation, along with reasoning, to MIS AVP/CIO to make a final determination. If a final determination is made by the MIS AVP/CIO to not recommend software, the MIS third-party management team will give potential alternatives to the requester. If final approval is given by the MIS AVP/CIO, the software will be added to AppLocker, so it can be installed/run.
2. **FREQUENCY OF SOP REVIEW**

The MIS AVP/CIO and CISO must review standard operating procedures annually, at minimum. This SOP is subject to revision based on the findings of these reviews.

1. **DOCUMENT ADMINISTRATION**

**DOCUMENT OWNER**

This document is owned by Management Information Services Office which is responsible for its content and maintenance. For questions or comments, please email prevattt@faytechcc.edu

1. **DOCUMENT REVIEW** **MANAGEMENT**

This document is subject to periodic review to validate the content remains relevant and up-to-date. Significant or material changes to this document must be submitted to the AVP/CIO for MIS and CISO for review and comment before adoption.

# **CHANGE HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Description**  | **Author**  | **Date**  |
| 1.0  | Initial publication  | Charity Banner | 12/05/2023  |

# **APPROVAL HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Name**  | **Title**  | **Date**  |
| 1.0 | Tenette Prevatte | AVP for MIS  | 12/2023 |