## How To:

## Implement Best Practices

## Purpose

The following checklist contains a list of best practices that should be followed in order to improve the security of endpoints and information belonging to users of the University of South Alabama.

## Checklist

### Ensure vendor software is up to date

#### Windows

- 1. Go to Windows Settings
- 2. Go to Update & Security
- 3. Check for Update

#### MAC

- 1. Go to Menu Bar
- 2. Select Vendor Software
- 3. Update

# Ensure operating systemupdates are set to automatically download and install Windows

1. Windows 10 users automatically receive updates by default.

#### MAC

- 1. Go to Apple Menu
- 2. Select System Preferences
- 3. Click "Check for Updates"
- 4. Install any pending updates

# Ensure third party applications and services are removed if no longer needed Windows

- 2. Review installed third party programs
- 5. Remove programs no longer needed

#### MAC

- 5. Go to Finder
- 6. Go to Applications
- 7. Review installed third party programs
- 8. Remove programs no longer needed

### Ensure third party applications and services are updated

- 1. Open third party application(s)
- 2. Check for Updates
- 3. If option not available, check application's website for latest version

#### Ensure firewall is ON for ALL networks

#### Windows

- 1. Go to Start
- 2. Search "Windows Firewall" under Control Panel
- 3. Select each network profile (Domain, Private, Guest)
- 4. Turn ON

#### MAC

- 1. Go to System Preferences
- 2. Go to Security & Privacy
- 3. Go to Firewall
- 4. Click lock icon in bottom-left corner: Enter credentials
- 5. Turn ON

## Ensure University-approved antivirus is installed

- 1. Uninstall all non-University-approved antivirus programs.
- 2. Download and install University-approved antivirus from:

1.

- 2. Go to https://www.southalabama.edu/departments/csc/informationsecurity/resources/encrypti onprocedure.pdf3. Follow instructions provided on the webpage