Desktop Security Checklist

This desktop security checklist consists of verifying computer security settings to determine if they are set appropriately and according to **PPM 10-1**, **PPM 10-3**, and the **Information Security Policy**. In addition, any cloud services are reviewed to determine compliance with **PPM 10-7**.

These requirements apply to faculty, staff, and all workstations. Exception forms are listed accordingly.

WSU Policies and Procedures Manual: Section 10 - Information Technology and Security

---

❐ **PPM 10-1, Information Security Policy and Computing Documentation Standard**

- **Verify the computer has the appropriate inventory tag.**
  - Items under $1,500.00 should have a purple tag;
  - Items over $1,500 should have a white tag
- **Verify the inventory tag is recorded**
  - Inventory is recorded on either the inventory list through Property Control (white tags) or in the PC Lifecycle database (purple tags)
- **Verify the computer name meets naming convention requirements**
  - (BldgCodeRoom#FullInventoryNumber- example: EH206-WS0123456)

Note: An exception request can be submitted using the form: Campus Name Standard Exception Request

❐ **PPM 10-1, Information Security Policy, Section O**

- Installed software is properly licensed

❐ **PPM 10-1, Information Security Policy, Appendix B**

- Automatic logins are disabled (only exception is kiosks). All other computers require a username and password to login.
- Sensitive information is secured when left unattended, both electronic and paper.
- Sensitive information is encrypted when stored electronically or hard copies are locked up.

- Users are not sharing their passwords
- Auto-lock feature is enabled and set to activate after no more than **20 minutes** of idle time. A password is required to resume activity once the auto-lock feature has activated (only exception is kiosks).
- Users should manually lock their computers when left unattended if it is visible to or accessible by anyone other than the authorized user.
- The university approved management policy framework is installed (currently this is System Center Endpoint protection) to manage antivirus and antispyware software.
- Anti-virus software is kept updated with the latest DAT files and antispyware software.
- A current operating system is installed and software updates are set to automatically download and install. ***(Note: a university wide exception was approved by the ISO office for lab computers.)***

❒ **PPM 10-1, Information Security Policy, Appendix B Continued:**

- Internet Information Systems (IIS) is disabled (not installed)
- Peer to Peer is disabled
- File and Printer sharing firewall exception is disabled for the home or work (private) network and the public network (the domain network should be enabled).

❒ **PPM 10-3, Network Security / Firewall Policy**

- Firewall is turned on

❒ **PPM 10-1, Information Security Policy, Section S**

- Any computing system that is unable to comply with this policy must file an exception. Exceptions to this policy must be approved by the Information Security Office based on academic or business need and will be reviewed by the Information Security Task Force.

Note: An exception request can be submitted using the form: Security Policy and Audit Exception Request

❒ **PPM 10-7, Cloud Storage and Application Policy**

Desktop Security Checklist

- All Users who utilize cloud services for storage and/or processing of University Business Information and/or Sensitive Information must utilize only University approved and contracted cloud services for such activities. Anyone wishing to utilize services outside of the University approved solution(s) must submit a copy of the contract for such services to the Information Security Office for review prior to purchase.
- University employees who are unable to comply with this policy must file an exception. Exceptions to this policy must be approved by the ISO based on academic or business need.

Note: An exception request can be submitted using the form: Security Policy and Audit Exception Request

---

Information Security Office (ISO)

Information Security Office: 801-626-6982 or security@weber.edu

Faculty and Staff can request assistance by contacting the Service Desk or their assigned CTC.

IT Service Desk at 801-626-7777 email csupport@weber.edu
Information Security Office at 801-626-6982 or security@weber.edu