The Texas A&M University System
Texas A&M Engineering Extension Service

Standard Administrative Procedures

29.01.03.N0.02 PC Management & Security

Approved: March 5, 2008
Revised: July 20, 2017
Revised: August 8, 2023
Next Scheduled Review Date: August 8, 2028

Summary

This SAP is intended to provide procedures to TEEX employees and Network & Information Services (NIS) to manage and secure TEEX personal computers (PCs). TEEX information resources are strategic and vital to the operation of the Agency. PCs are an integral and key component of the Agency’s information infrastructure. These procedures are essential to protect PCs and their data against unauthorized access, disclosure, modification, or destruction (accidental or deliberate).

Definitions

PC means personal computer regardless of manufacturer or operating system, and therefore includes any single-user desktop or portable computer (including netbooks), tablets or smartphones.
TAC is Texas Administrative Code.
TAC 202 is Texas Administrative Code Title 1, Part 10 Chapter 202 Information Security Standards. It contains administrative rules for Texas Agencies and Institutions of Higher Education.

Requirements

1. Replacement Cycle Management

1.1. A recommended PC replacement schedule helps to ensure that PCs are not retained past the end of their economic life. Due to continual advances in software and hardware technology, there comes a point at which the cost of continuing to support and maintain obsolete PCs exceeds the long-term benefit to TEEX. Industry guidelines vary, but the range of recommendations is between 3 and 5 years.

1.2. TEEX has adopted 5-year service life as the maximum age for personal computers as long as the computer is still capable of meeting all security requirements. Any exceptions to service life and security requirements must be requested through the NIS Security Exception Form.

1.3. Divisions/departments shall surplus PCs following the Financial Services Surplus of TEEX-owned Technology Equipment guideline as defined in TEEX SAP 21.01.09.N0.01

Property Acquisition, Responsibility, and Accountability which provides special instructions on disposing of PCs.

2. Administrative Management

2.1. The assigned "Computer Name" shall not be changed by a user. This name is comprised of the PC's TEEX asset tag number, preceded by a "T" (i.e., T716xxxx), or other NIS designated device name.

2.2. "TEEXAdmin" and "TEEXUser" accounts/passwords shall not be changed by a user.

2.2.1. TEEX employees shall use the account issued to them for normal activity.

2.2.2. TEEXUser should only be used on PCs authorized for shared use (for instance PC located in conference rooms or training rooms).

2.3. When a PC is reassigned to a different employee, the division/department should request that NIS re-image the PC to:

- Remove the previous employee's files,
- Ensure that the latest software and updates are installed, and
- Provide "like-new" PC performance.
- Comply with any data preservation requirements.
- Comply with any special security requirements (i.e. CUI), contractual security requirements, non-disclosure agreements, etc.).

Exceptions may be granted on a case-by-case basis and must be routed through the NIS Security Exception Form.

3. Software Installation and Support

3.1. All new and reimaged PCs configured by NIS will have TEEX standard software installed. The TEEX standard software includes Windows OS, Microsoft Office, and Adobe Acrobat Reader. Any other nonstandard software that needs to be installed will need to be requested. In some cases, some nonstandard software installation request requires an approval by the TEEX Information Security Officer via the non-standard software request form.

3.2. NIS provides technical support for TEEX standard software as indicated in the authorized software list. NIS provides limited technical support for nonstandard software installed on PCs. In some cases, Divisions/Departments need to purchase maintenance and support contracts on nonstandard software for technical support and software update.

3.3. Software may be periodically added or removed from the authorized software list.

4. Updates and Security

4.1. All TEEX PCs shall have the current management and security software installed. All management and security software must not be removed or disabled.

4.2. Each user is responsible for ensuring operating system and any installed software are up-to-date, in accordance with the SI-2 Flaw Remediation in the Security Control Catalog, on all PCs assigned to them on their respective Property Accountability form.

4.3. With the exception of PCs used to deliver training and/or technical assistance products and services to TEEX customers, all TEEX PCs shall be set with a password-protected screen saver timeout set to automatically lock the workstation after 15 minutes of inactivity. Any other exceptions must be routed for authorization through the NIS Security Exception Form.

4.4. The above requirements apply to all TEEX PCs, including those not currently in use. Any other exceptions must be routed for authorization through the NIS Security Exception Form. This means any and all stored or cached PCs hat are not regularly connected to the network must be connected to the network and powered on to allow updates and monthly automation to occur.

4.5. NIS makes efforts to automatically update OS and agency standard software if the machine is connected to the network and left on for normally expected office usage. PCs should be rebooted on at least a monthly basis to aid with the automation.

4.6. Divisions/departments are responsible for updating all agency standard and nonstandard software and removing unused software not acquired through NIS, to include trials, freeware, and browser extensions.

4.7. Employees shall report any observed or suspected security non-compliance immediately via email to security@teex.tamu.edu or helpdesk@teex.tamu.edu.

Quality Assurance Measures

NIS monitors installed software and version installed via automation. When notified by NIS to correct a compliance issue with an assigned PC, a user has 10 working days to ensure non-compliance issues are satisfactorily resolved. In the absence of a response from the user within 10 working days, the non-compliance issue will be referred to the Division Director. If the issue remains unresolved after 5 additional working days, NIS may block the PC and the assigned user from the network. This action is required to mitigate the risk to the entire network by a single non-compliant PC.

Related Statutes, Policies, or Requirements

System Policy 29.01
System Regulation 29.01.03
Texas Administrative Code: Title 1, Part 10, Chapter 202, Subchapter C (TAC 202)
TEEX Security Control Catalog

Office of Responsibility

Network & Information Services
(979) 458-6868