

# Low-Cost/No-Cost Computer Security Measures

---

## System Monitoring

1. Ensure system audit features are active on the system.
2. Protect the audit trail so that no normal user can view or modify the audit log.
3. Do not allow multiple logons. If an employee is allowed to logon to his/her workstation and then walk around the corner and logon to another workstation with the same logon ID and password, the audit trail can no longer track the user as precisely as security needs require. If both terminals are active with the same logon, the system can never be sure if the authorized user is on the system or if someone else is using his/her account.
4. Review audit trails for security-related incidents as well as for “health” of the system on a regular basis (daily if possible).
5. If the option exists, display, with a pause, the last unsuccessful logon attempt on the workstation screen.
6. Do not allow sniffer boxes to run unattended or unsecured.
7. Provide all users of the system with “security alert” announcements.

---

## General Security Administration and Awareness

1. Assign a system security officer to each computer area and set of workstations.
2. Provide adequate training for all system administrators, system security officers, and LAN maintenance personnel.
3. Implement a security awareness program. The program should include orientation for new users as well as annual training for veteran users.
4. Turn on security features provided by the system vendor.
5. Develop a prioritized list for security enhancements/upgrades.
6. Ensure that all users know the correct procedure for reporting security problems. This can be part of the annual security training program.
7. Ensure that all users know what to do with their computers and media when responding to a fire alarm or other emergencies requiring evacuation.

8. Establish and regularly review policies and procedures for equipment maintenance and physical security.
9. Ensure that all users understand the policies and procedures for moving data from one system to another, particularly if the systems operate at different levels of sensitivity/classification.
10. Ensure all users know the current policy on reuse of computer components and magnetic media.
11. Employ warning banners that cover security and other issues of concern.<sup>1</sup>
12. Standardize account request forms and procedures to simplify audit reviews.
13. Standardize help desk verification and account reset procedures.
14. Establish end-of-day procedures for closing down individual work areas.

---

## **Access Control**

1. Direct users to lock their computer screens every time they leave their computers. Never give someone (who may not have file access privileges) the opportunity to use an account other than his or her own: it negates the use of audit trails for tracking. Use a password-protected screensaver initiated by the user or activated after a specified period of inactivity.
2. If logon sessions are inactive for more than 10 minutes, lock the screen or account. The owner will have to enter his/her password to unlock the screen/account.
3. Secure all removable storage media at the end of the day.
4. Delete all guest accounts. When a guest needs the use of a computer, establish a new account and password with proper access controls. When the guest leaves or no longer needs the use of the computer, delete the account immediately.
5. When a user changes jobs, retires, quits, or is terminated, delete all affected accounts immediately. If necessary, disable the account for a set period of time (e.g., three months) to allow coworkers to access it for documents or e-mail related to ongoing projects. After a set period, purge the account from the system.
6. Keep access privileges (read, write, exec, etc.) current and limited to the minimum required to do the job.
7. Verify that physical access security devices for computer facilities are current. This includes keeping tables for badge swipes up to date and changing door combinations when required.

---

<sup>1</sup> See 1 TAC 202.25(9) and 1 TAC 202.75(9)

8. Control access to the computer room. Escort outside maintenance personnel and other visitors.
9. Verify, on a regular or random basis, that firewall or router IP access control lists are accurate and current.
10. When using office-issued laptops, be sure to handle and maintain them properly.

---

## **Configuration Management**

1. Ensure that system documentation such as security plans, concepts of operations, and configuration management plans contain an accurate description of all interfaces with other systems, sites, or agencies.
2. Eliminate all connections to critical systems that are unrelated to their primary functions.
3. Know what hardware and software is on the system/network. Establish a Configuration Control Board or process for tracking hardware/software in place and for installing and testing patches and upgrades on a timely basis.
4. Limit authority for adding new software or upgrading current software to system administrators.
5. Use modems only when necessary, preferably in a modem pool configured to be outside the firewall (see Access Control in Chapter 3). Turn off modems when not in use, and disconnect them when practical and/or possible.
6. Do not make the Web server part of the network (local or wide area). A Web server on the network could provide an additional path to protected information.

---

## **Protection of Information**

1. Know the value of the information being processed and why it should be protected. Add this information to security awareness training for the new user as well as the annual security awareness training program.
2. Eliminate storage of critical information at local workstations, to reduce both the chance of unauthorized access and the chance of accidental loss or destruction (for example, from a hard drive failure).
3. Make regular backups of data files and system files.
4. Store backup files securely offsite, in a location from which they can be retrieved within the time required for resuming system operation.
5. Use antivirus software that contains a virus scanner. Scan *all* files entering the system, not just files from across the Internet.
6. Always use the latest version of the authorized antivirus software.

7. If users work outside the office and bring their output to work on disks and diskettes, require scanning of all such removable storage media before files are copied to an office workstation or laptop.
8. Label all removable storage media that contains sensitive or critical data.
9. Dispose of damaged removable storage media appropriately.

---

## **Disaster Recovery<sup>2</sup>**

1. Make sure there is a disaster recovery plan in place.
2. Test the disaster recovery plan at least once a year. If it is not practical to test the plan by shutting down the entire system, test it module by module, while the rest of the system remains in operation.

---

<sup>2</sup> See 1 TAC 202.24(a)(5) and 1 TAC 202.74(a)(5)