

Information security violations can happen anywhere to anyone. It is the responsibility of each DAS employee to protect the information technology (IT) resources we use every day. Proactive daily work habits can help you protect the IT resources that DAS has entrusted to you.

Computer guidelines:

- Do not share your computer, network and/or application (Outlook, OAKS, etc.) passwords except when working with the DAS IT Services staff.
- Do not use simple, obvious, or predictable passwords. For example, do not use the names of relatives or pets; nicknames; days and months; repetitive characters, etc.
- Be creative when selecting passwords. Strong passwords use a minimum of eight characters and include a combination of symbols, numbers, upper and lowercase letters.
- Do not write down your passwords or post them on your terminal or other obvious places. Don't create macros or other shortcuts to record your passwords.
- Do not use the "save password" option when using web-based applications.
- Change your passwords if you suspect that any of your passwords are known to someone else. Notify your supervisor.
- For new employees, always change the initial password assigned to you by DAS IT Services as soon as you receive it.
- Change your passwords in accordance with the schedules established for the computers, networks and applications that you use.
- Do not use someone else's Login ID and password. If you are having problems with your access, contact DAS IT Services.
- Do not use your access privileges to enable others to access information that they are not authorized to access or to submit transactions that they are not authorized to submit.
- When leaving your workstation area, lock your computer (press CTRL + ALT + DELETE) then click on "lock your computer." If your workstation is located near a public area, lock your computer if you are stepping away from your desk, even momentarily. Your computer will automatically lock after 15 minutes of inactivity. Remember – Lock it when you leave it!
- At the end of your workday, shut down your computer. This shut down heightens security, reduces energy usage and enables DAS IT Services and OIT Network Services to deploy updates to your computer.
- Secure all portable devices (i.e., CDs, disks, flash drives, etc.) and store those containing sensitive information in a safe environment. Consult with your supervisor before removing a portable device from your work location.
- Consider electronic documents and e-mails that are part of official files for record retention before erasing old files and documents. Consult with your supervisor and/or DAS legal counsel for guidance.
- All files should be stored on network drives for backup purposes. Personal files should not be stored on network drives.
- For DAS employees with web-based access to the state's computer systems, seek guidance from the DAS IT Services before accessing information using wireless, satellite and other evolving technologies.

- Work with DAS IT Services to arrange for installation of software. Only IT Services desktop staff are authorized to load software onto an employee's computer.
- Assistance for the above issues is available through the DAS IT Services Help Desk at <http://apps.intranet.das.ohio.gov/helpdesk/logon.asp>

Internet, e-mail and other IT resources guidelines:

- For full details, refer to DAS IT Resource Usage Policy (700-01) and the State of Ohio IT Policy, ITP-E.8, Internet, E-mail and Other IT Resources.
- Do not open (i.e., view, detach or launch) suspicious e-mail attachments.
- If you receive a suspicious e-mail attachment, contact your DAS IT Services desktop representative immediately. Do not send a copy – verbally provide your name, the sender's name, date, and name of attachment.
- If you receive an unexpected or suspicious e-mail from someone you know, contact the person who sent you the attachment to verify that they actually sent it and immediately contact the DAS IT Services Desktop staff.
- Do not configure your e-mail to automatically open attachments. If your e-mail program automatically opens attachments, disengage it or contact your DAS IT Services technician for assistance.
- Ensure confidential or sensitive information on DAS systems is protected with an effective authentication mechanism, encryption software or firewalls. Ensure your DAS IT Services representative knows the existence and location of confidential and sensitive information.
- Be familiar with ITP-E.8, Section 5.2, Unacceptable Personal Use policy. Any personal use of IT resources that disrupts or interferes with government business, incurs an undue cost to the state, could potentially embarrass or harm the state, or has the appearance of impropriety is strictly prohibited. Personal use that is strictly prohibited includes, but is not limited to: violations of law, illegal copying, operating a business, accessing personal services, accessing sexually explicit material, harassment, gambling or wagering, mass e-mailing, solicitation. See ITP-E.8 for descriptions of each prohibited activity.
- Take all reasonable precautions to prevent the inadvertent dissemination of anyone else's information via the Internet, electronic mail or online services.
- State employees have no reasonable expectation of privacy in conjunction with their use of state-provided IT resources. Contents of state computers may be subject to review, investigation and public disclosure. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by state or federal law. Web browsers leave traceable "footprints" to all sites visited. The state reserves the right to view any files and electronic communications on state computers, monitor and log all electronic activities, and report findings to appropriate supervisors and authorities. See ITP-E.8, Section 5.6.
- Also, see Procedure C-4: Cyber-attacks.

Paper documents and file guidelines:

- Do not leave sensitive or confidential information lying around. File or dispose of sensitive or confidential information properly and timely.
- Store valuable information in a secure location such as a locked desk, cabinet, or office.
- Label your paper files for identification and store sensitive files in a secure location. If portable devices (disks, CDs, etc.) are included as part of a sensitive file, be sure to encrypt or password protect these portable devices. Personally owned flash (USB) drives are not

permitted to be used with DAS computers or laptops. If flash drives are necessary in order to do your job, only a state-owned fully FIPS 140-2 compliant flash drive is permitted to be used. For questions regarding flash drive usage, please consult DAS IT Services.

NOTE: This procedure provides limited guidance to heighten security awareness with regard to computer usage, Internet usage and information. For a complete policy regarding IT Resource Usage, please visit <http://das.ohio.gov/Divisions/AdministrativeSupport/EmployeesServices/DASPolicies/tabid/463/Default.aspx> and click on Policy 700-01 entitled IT Resource Usage Policy. OIT also maintains statewide policies for state agency usage entitled: Use of Internet, E-mail and Other IT Resources (ITP-E.8), Internet Security (ITP-B.6) and Electronic Records (ITP-E.30) which address building and managing Internet servers and electronic mail services, and personal responsibility of state employees using the Internet, electronic mail services and online services. These and all other statewide security policies can be found at <http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx>

DAS IT Services provides additional guidance on IT privacy and security-related issues through the periodic release of Informational Bulletins. These bulletins are available on the DAS website at the following link: <http://das.ohio.gov/ITSecurityPrivacyAwarenessProgram/tabid/460/Default.aspx>