INFORMATION, NEWS, AND SUPPORT
Information Security Shared Services

2nd Edition
October 2016

Cyber Security Bulletin

Clear Desk, Clear Screen Tips

Information must be protected, both inside and outside the office, from unauthorized access at all times. Many offices are open to the public, and potentially, to prying eyes that should not have access to confidential or sensitive information. Employees travelling or teleworking may inadvertently expose confidential or sensitive information. Maintaining clear desk and clear screen practices helps ensure information is not exposed to people who happen to be walking by or those who intentionally seek to steal information. Here are some tips that all employees should follow to protect confidential and sensitive information:

WORKSPACE: Don't leave confidential or sensitive information exposed when you are not at the desk or where others passing by your desk can view it. Lock information in a drawer or cabinet when not being used or when you are away from the desk.

USER CREDENTIALS: Don't write down your user name, password or other sensitive information on a post-it-note and post it around your work space. Memorize the information or use a secure password manager such as LastPass.

COMPUTER SCREEN: Always lock your computer when you are leaving your desk; even for a short time. For example, on a Windows computer you can press Ctrl+Alt+Del on your keyboard and select to lock the computer (or use Windows Key + L). Don't depend on the auto lock feature on the computer as someone could access it before the auto lock takes effect.

More clear desk, clear screen tips

1) **REMOVABLE STORAGE MEDIA:** Don't leave removable storage media plugged in or lying around for unauthorized employees or visitors to access. Removable media may include CDs, DVDs and USB drives. Lock away removable media when not in use. Encrypt all confidential and sensitive information stored on removable media.

2) **PRINT OUTS AND COPIES**: Don't leave documents sitting on a copier or fax machine. This is a very common way confidential and sensitive information is exposed. Collect documents from the printer as soon as you print them and always pick up originals from the copier or fax machine.

3) **INFORMATION DISPOSAL**: Never throw out documents with confidential or sensitive data into a trash can. "Dumpster Diving" is a popular method of stealing information. Documents should be shredded or disposed of according to your college data retention policy.

4) **PORTABLE DEVICES**: Portable devices such as laptops and tablets should always be locked away when not in use. Always use password protection on portable devices!

Virginia's Community Colleges

VIRGINIA WESTERN
Celebrating 50 Years