

INFORMATION SECURITY AWARENESS TRAINING

Version: 1.0

Status: Approved 09/26/07

Contact: Director, Technology Services

PURPOSE

This guideline provides high level security awareness training information to address one of the provision of the COV Security Standard which require all individuals having access to the Commonwealth's IT resources to complete security awareness training.

SCOPE

This guideline is applicable to the provision of adequate Security Awareness Training.

APPLICABILITY

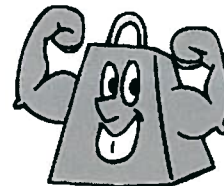
This guideline is applicable to all System Office, third party consultants, and short term employees.

GUIDELINE

The following information must be reviewed and signed by the consultant/3rd party employee and the System Office staff member responsible for supervising their activities.

Information security is everyone's responsibility.

1. Sensitive enterprise information or personal information (financial, health, grades, etc.) must be protected and secured from unauthorized access and unintentional damage.
2. Electronic information now extends far beyond traditional mainframe systems, web servers, e-mail servers, and desktop computers. Information security requirements now extend beyond our organization's physical walls. Electronic information is available on many different portable devices, in many different places and with many different people. We are all responsible for safeguarding such devices.
3. Non-electronic information is just as valuable as electronic information and just as difficult to protect from unauthorized access or information breaches. Roles and responsibilities are vital to ensure that all types of non-electronic information are protected.
4. Passwords are one of the first layers of protection. Passwords should never be shared and should always be kept confidential, just like your personal identification number (PIN) to your financial accounts. While passwords can be one of the weakest links in an information security/privacy program, passwords are not as difficult as you might think.
 - a. Passwords are important to prevent unauthorized access to systems and information.
 - b. Passwords are important to prevent unauthorized access to encryption keys that protect information.
 - c. Changing passwords routinely is important to prevent unauthorized access by someone that may have stolen or guessed your password.
5. Strong passwords should include the following characteristics:
 - a. Consist of 6 or more characters
 - b. Use special characters such as #, \$, %, ^ (if allowed by your system)
 - c. Use one or more spaces (if allowed by your system)
 - d. A mix of uppercase and lowercase letters
 - e. A mix of both numbers and letters



6. Users and organizations must improve their Internet security awareness to prevent Internet abuse and incidents related to:
 - a. Inappropriate content (pornography, pirated software, etc.)
 - b. Non-business web sites (video, music, sports, gaming, etc.)
 - c. Games, jokes and chain letters
 - d. Illegal software sharing
 - e. Etiquette and professional behavior with E-mail, text messaging, and other messaging services.



7. Please remember; the Internet is not as anonymous as you thought it was.
8. E-mail and system best practices that will help avoid viruses, worms and spyware include:
 - a. As attackers continue to create new viruses and attacks, it is important to keep your anti-virus software current.
 - b. Use and update anti-spyware software that is capable of identifying and removing spyware and other crime-ware that is detected on your PC or systems.
 - c. Change your passwords if you experience a virus, worm or spyware outbreak as your passwords may have been compromised during the infection. It is suggested that web site passwords are also changed and you should use strong passwords that are difficult for attackers to guess.
 - d. While most organizations utilize a company-wide firewall, utilizing a hardware or software firewall on your laptop or home PC can help to prevent security risks by blocking malicious threats before they can cause problems.
 - e. Make sure your e-mail systems and browsers are configured to provide security at appropriate levels and patched with the latest software updates and fixes.



9. **Social Engineering** is one of the oldest and one of the most effective methodologies for hacking and stealing sensitive information. Social Engineering is a social attack, or an attack focused at people. To launch a social attack, an attacker uses human interaction (social skills) to gather or compromise sensitive information about a person, an organization or a system.
10. People play a very important role in Incident Management and must understand the importance of paying attention to surroundings, applications, information handling and infrastructure performance to notice potential incidents. A few examples of suspicious activities that could indicate a social hacking incident include:
 - a. Are you receiving phone calls from individuals requesting information about your login or passwords?
 - b. Have you noticed a stranger or new people working in your area?
 - c. Is your work area missing any paper documents, manuals, CDs or backup devices?
 - d. Have you noticed cleaning crew personnel spending extra time in offices, work areas or around systems?
 - e. Have you noticed any employees working unusual hours or behaving inconsistently with what might be normal for those employees?
 - f. Have your e-mails been opened or changed before you accessed them?
 - g. Have you heard anyone talking about strange system changes, phone calls or e-mails?
 - h. Have customers had to resend information to your attention?
 - i. Have you noticed that your system has changed or new icons/ programs have been added to your PC screen?

11. All employees, consultants, and visitors are expected to review and adhere to the VCCS Information Security Standard, acceptable use agreements and related standards. You will find this information at the following web link:
<http://www.vccs.edu/FacultyStaff/InformationTechnology/Standards/tabid/357/Default.aspx>).

LET'S ALL BE AWARE AND ADOPT SECURITY BEST PRACTICES TO SAFEGUARD VCCS IT SYSTEMS, DATA AND RELATED RESOURCES!!!!!!

Employee/Consultant Name (Print)	Project/Work Department Sponsor Supervisor Name (Print)
Employee/Consultant Name (Signature)	Project/Work Department Sponsor Supervisor Name (Signature)
Date	Date