West Virginia State Government
Executive Branch
Information Security
Best Practices Summary

A Summary Guide for All Computer Users

Background:

For the last 20 years Information Technology (IT) has assumed an increasingly vital role in the workplace. West Virginia State government cannot operate successfully without reliable systems, and accurate data. Without computing resources, all business, as we now know it, would suffer. Along with the powerful advantages provided by computer networks, the Internet, and global connectivity, real risks exist that require **every user to assume a role in computer security**.

Information Security policies, procedures, and practices address 3 key goals: (**C)onfidentiality, (I)ntegrity, and (A)vailability**. This means: **(C)** Keeping data from unintended or unlawful exposure; **(I)** keeping data accurate; and **(A)** keeping computing resources always available for necessary use. Remember **CIA**. In order to keep information secure, **standard procedures** must be followed:

Standard Procedures / Best Practices:

Confidential Information: Never leave confidential information lying around face-up where it can easily be viewed. Printers and FAX machines are places to watch. Best Practice: Confidential information should be secured. **Proper disposal** of information (paper, hard drives, diskettes, CDs) is critical to the **safeguarding of data right to the end of its lifecycle.**

Unattended Workstations: Always secure your computer (Lock using Windows Key-“L”) when you leave your computer, even for a moment! When someone else uses your logged-on workstation, it appears as if it is you. You are responsible.

Saving Data: **Always** Save **all** important data to a **server drive.** Your C: drive (the drive in your PC) is **not** backed up.

Passwords: Passwords must be created that cannot easily be guessed. **Strong passwords** have three of the four character types: lower case, UPPER CASE, numb3rs, and $ymbol$. Longer is better. 8 character minimum. Strong Password example: “At one time nobody had to lock their house” = @1Tnh2lth

1) Passwords must never be shared, even with a secretary or a supervisor or manager. The OT Service Desk will not ask, nor will a technician.
2) Passwords must never be written down and stored where others can easily find them.
3) Passwords must be changed on a regular basis (35 days max.) because a stolen password file can be decrypted by a fast computer after a number of days, allowing unwanted illegal and malicious access to systems.

Threats: Viruses, Worms, Trojans, Zombies, Spyware, Spam, Phishing, etc.:

1) These common threats represent challenges_to Information Security, and often cause_computer problems that require costly_technical reworking. The problem worldwide_is expensive – in the $Billions annually.

2) Most of these types of threats are associated with **e-mail,** or **WEB access,** and can be avoided. They can stop your computer from working, and cost you lost time, missed deadlines, and possibly worse.

i) Never open an e-mail attachment that is from an unknown source, or that was unexpected.

ii) **Phishing:** Never click on a link embedded in an unsolicited e-mail that asks you to go to a site and provide personal information to resolve a “compromised account.” This is a common exploit used for identity theft, and leading to financial loss. Phishing that targets individuals known to have valuable assets is called “spear phishing.” Avoid WEB sites that are unrelated to legitimate business. Offers of gifts are usually designed to obtain information for sales purposes, called SPAM. Usually there are lots of questions asked.

Never impair installation of new security updates and anti-virus signatures that are downloaded to your computer!

E-mail and Internet Use:

1) E-mail and the Internet are provided at work for business purposes, and should be limited to very minimal personal use during break times, like the telephone. No non-State email systems should be accessed.
2) E-mail and Internet access should never be used for unlawful purposes, or for purposes that could be viewed as improper or unethical for a work place and work time (e.g. chain letters). If in doubt, ask your IT contact.
3) Ignorance is not an acceptable excuse for misuse, and some misuses can lead to discipline or dismissal.
4) All use is subject to detection. Nothing can ever truly be deleted from a computer. **Be smart, be careful … and be aware!**

Streaming Audio and Video / Downloading / Non–business software / Attaching to the Network:

1) Streaming audio and video must only be used for business purposes, since it uses considerable communications bandwidth (network capacity). No Internet radio is permissible.
2) Downloading music, software, or other unauthorized content is explicitly prohibited.
3) Installing programs not owned or authorized by the State onto a State computer, is prohibited.
4) File sharing programs (e.g. Kazaa, Limewire) and unauthorized Instant Messaging (IM) are not permitted.
5) Don't install hardware and software yourself. Leave that to your Office of Technology support person.

Laptops, Notebooks, Tablets, Personal Digital Assistants (PDA), Cell Phones, “Smartphones,” USB Drives, etc.

These devices have monetary value, and often contain sensitive data. They should use encryption when private or legally protected information is stored in them; should have anti-virus protection installed, have firewall software installed, and never be left in plain view in automobiles, or in places where theft or heat damage is likely. In summary, good Information Security practice is often simply ***common sense***. **Please diligently safeguard State computing and information assets and resources.**

If you ever have a question, or an incident to report, contact Harlan White at Extension 2002 or whiteh@wvlc.lib.wv.us

Report incidents quickly!

Acknowledgement: I acknowledge that I have read and understand both the concepts presented in this Information Security Practices Summary, and the expectation that I will comply with them.

Name: ________________________________

Date: ________________________________

Do your part keep “IT” secure!

Understand and comply with WV Information Security Policy, online at:
http://www.state.wv.us/ot/PDF/Document_center/ SecurityPol0107.pdf

*** ** SAFEGUARD STATE INFORMATION ASSETS *****