

"Cyber Security Awareness" is the knowledge that VA volunteers utilize to protect VA computer systems and data. It is more than policies, procedures, rules, and regulations. Cyber Security Awareness refers to the personal responsibility each of us assumes for ensuring:



- the confidentiality, integrity, and appropriate availability of Veterans' private data,
- timely and uninterrupted flow of information throughout the VA enterprise, and
- VA information systems are protected from the potential of fraud, waste and abuse.
- Please be aware of any activity that might violate and/or compromise the security of VA

information systems. Report all incidents to your information security officer.

Know Your ISO

- Do you know all the rules and requirements you should follow to keep VA's information secure?
- Do you know what to do if your computer is infected with an electronic virus?
- If you witnessed someone using VA's computers for theft or fraud, what would you do?
- Do you know your responsibilities for maintaining confidentiality and privacy?
- Are you sure that your work is backed up and safe?
 - Do you know your role in your facility's contingency plan?



There is someone available to help you - your facility Information Security Officer. Robert Barnhart is the Information Security Officer for the Chillicothe VA Healthcare System. His phone number is 740-772-7071.

Passwords

Passwords are important tools for protecting VA information systems and getting your job done. They ensure you have access to the information you need. Keep your password secret to protect yourself and your work.

Passwords must:



- Be constructed of at least eight characters (i.e., Gabc123&).
- Use at least three of the following four kinds of characters:
 - Upper case letters (ABC...)
 - Lower-case letters (...xyz)
 - Numbers (0123456789)
 - "Special characters," such as #, &, *, or @.
- Be changed at least every 90 days.

Incidents

Take a few moments to consider how important VA's computers are in conducting our business. Almost everything we do depends on our computers. Unfortunately, the same computers that



help us serve Veterans can also be used for theft and fraud. Electronic viruses can attack our computers. They can be stolen and vandalized. They can be used to distribute sensitive information to those not authorized to receive it. All these are examples of computer-related incidents. It is important to let your supervisor and Information Security Officer (ISO) know when you witness such incidents. Your ISO will contact the VA Security Operations Center (SOC) (VA SOC). Reporting cyber security incidents helps VA to reduce the negative impact of these events and to improve VA's information

processing ability.

The VA SOC was established to fulfill VA's need to ensure that computer security incidents are detected, reported and corrected as quickly as possible, and with minimal impact. VA SOC's primary responsibilities are to:

- Serve as a central clearinghouse for all reported incidents, security alerts, and notifications;
- Ensure additional SOC resources for all VA incidents as needed;
- Coordinate effective notification of and response to all reported incidents;
- Notify proper officials in each organization of reported incidents.

Incident Do's and Don'ts

may



involved computer systems.

- Describe what you believe happened.
- Copy any error messages displayed on your computer screen.
- Copy any involved web addresses, server names, or IP addresses.

When you think a computer security incident have occurred, you should

- Gather details of the incident so you can communicate specific information to your ISO.
- Collect the date, time, location, and

Time may be of the essence. You may need to contact your ISO by phone or in person.

Do not discuss the incident with the media (radio, TV, newspapers) or anyone outside of your facility without first consulting your ISO and facility management.

To report a cyber security problem, your primary point of contact is your VA information security officer.