

VA Information Security Awareness Course



October 1, 2008

Developed by US Department of Veterans Affairs, Office of Information and
Technology, Office of Cyber Security, Education and Training Division

Table of Contents

Welcome.....	3
Course Objectives	5
Course Outline.....	6
Introduction	7
Know Your Information Security Officer (ISO).....	8
Confidentiality.....	9
Ethics.....	13
Knowledge Check 1	14
Authorized Use of Equipment.....	15
Knowledge Check 2	20
Email	21
Knowledge Check 3	26
Remote Access	27
Removable Storage Media	28
Knowledge Check 4	30
Malware.....	31
Knowledge Check 5	38
Social Engineering	39
Public Peer-to-Peer File Sharing.....	43
Knowledge Check 6	45
Wireless Network Security.....	46
Laptop Security	49
Knowledge Check 7	50
Passwords	51
Backups	57
Knowledge Check 8	60
Incidents	61
Rules of Behavior.....	65
Final Summary	68
Knowledge Check 9	70
Department of Veterans Affairs (VA) National Rules of Behavior.....	72

Welcome

Page 1 of 2

Audio:
None

Text:
The Awareness Course

Welcome to the Information Security Awareness Course. This course will take approximately 60 minutes to complete. You are here because Congress mandates that all VA employees, contractors, and all other users of VA information and VA information systems complete computer security training. At completion you will have a deeper understanding of practices that can drastically reduce chances of a security incident happening.

This training focuses on important security practices and procedures. It includes information that VA employees, contractors, volunteers, students, Veterans Service Officers, and State Veterans Assistance Office staff need to know in order to protect information about veterans.

If you are taking the paper version of the course, you will need to work with your supervisor and LMS administrator to ensure you receive credit for completion. Additionally, you need to print out and sign the VA National Rules of Behavior at the end of this course. You will need to print and sign two copies of the Rules of Behavior. One copy needs to go to your supervisor and you need to keep the second copy for your own records.



Welcome

Page 2 of 2

Audio:
None

Text:
Why We Have to Complete This Each Year

Annual security awareness training is a Federal Information Security Management Act (FISMA) 44 USC 3544(b)(4) requirement. Completion of this course meets the requirement.

Mandatory training related to these laws includes the following required tasks by all VA employees:

- Compete Annual Information-Security Awareness Training
- Complete Annual Privacy Awareness Training
- Read and sign the VA National Rules of Behavior annually

Failure to comply with the above will result in denial or removal of access rights and privileges to VA information and information systems, which may have an adverse impact on the performance of duties.



Course Objectives

Audio:

None

Text:

Upon completion of this course you will:

Know when to contact your Information Security Officer

Know elements required for a secure password

Recognize VA sensitive information

Be aware of VA policies to protect information

Be aware of information security requirements to protect an individual's privacy

Be aware of the importance of backups

Be aware of the potential dangers of using e-mail

Be aware of the potential danger of using a wireless network

Know how to report suspicious incidents to your ISO

Be aware of how important VA information is to the Government and veterans

Be aware of the difference between the use of VA information resources in your work setting versus for your personal use

Understand the VA National Rules of Behavior



Course Outline

Page 1 of 1

Audio:

None

Text:

The following topics will be covered in this course:

Know Your Information Security Officer (ISO)

Confidentiality

Rules of Behavior

Ethics

Authorized Use of Equipment

Email

Remote Access

Malware

Social Engineering

Public Peer-to-Peer File Sharing

Removable Storage Media

Wireless Network Security

Laptop Security

Passwords

Backups

Incidents

Introduction

Audio:

Welcome to the information security awareness course. In the next hour you will review your role in protecting the information of our nation's veterans.

Text:

Information Security Awareness helps protect VA information and information systems. It is more than policies, procedures, rules, and regulations. Information Security Awareness helps you understand what you need to do to ensure:

- Confidentiality, integrity, and availability of veterans' Sensitive Personal Information (SPI)
- Timely and uninterrupted flow of information throughout VA systems
- The protection of VA information and information systems from fraud, waste and abuse

Much of what you learn in this course will not only help you protect VA information, it will also help protect you as a computer user. If you suspect VA information or VA systems have been violated or put in danger (compromised), report this to your Information Security Officer (ISO).



Know Your Information Security Officer (ISO)

Audio:

If you have any questions regarding information security, always start with your ISO.

Text:

Your ISO is there to help you understand the rules and requirements to keep VA's information and systems secure. Your ISO can help with issues such as:

- Knowing what to do if your computer is infected with a virus

- Knowing what to do if you see someone using computers inappropriately or for theft or fraud

- Understanding your role in protecting the confidentiality and integrity of VA's information

- Understanding how backups are conducted and why they are important

- Knowing your role in your facility's contingency plan

Every VA facility has an ISO, who can help you with issues like those above. If you do not know your ISO, ask your supervisor or visit the VA Information Protection Portal for the ISO Directory.



Confidentiality

Part 1 of 4

Audio:

One of your most important responsibilities is keeping VA information confidential.

Text:

Confidentiality at VA means information is available only to those people who need it to do their jobs. At VA, confidentiality is a must.

To maintain confidentiality:

- Understand what information you have access to and why.
- Read and follow remote access security policies.
- Only access information systems through approved hardware, software, solutions, and connections.
- Take appropriate steps to protect information, network access, passwords, and equipment.
- Don't using automatic password-saving features found on web sites.
- Promptly report to your ISO any misuse of the remote access process or report if VA sensitive information has been compromised.
- Understand the National VA Rules of Behavior



Confidentiality

Part 2 of 4

Audio:

There are some simple rules that go a long way towards keeping VA's information secure.

Text:

To maintain confidentiality:

- Lock your computer (Press **Control, Alt,** and **Delete** at the same time, then select **Lock Computer**) when you walk away from it. This will prevent an unauthorized user from performing tasks or accessing information using your account.
- If you print VA sensitive Information, make sure you take it from the printer right away and keep it stored in a secure place.
- Protect all information and only access information you need to do your job.
- Never talk about a veteran's case in a public place or to anyone who does not have the need to know.
- Never take VA sensitive information home unless you have your supervisor's and ISO written permission.

VA computers are set up to protect confidentiality. But you also have to do your part.



Confidentiality

Part 3 of 4

Audio:

More confidentiality issues arise when it is time to retire old computer equipment.

Text:

How would you feel if your personal information was stored on a computer, and then the computer was given to another person? This would be a breach of your confidentiality and you wouldn't like it. To prevent this, the VA has strict guidelines in place to ensure the proper sanitization and disposal of media containing VA sensitive information. There is a media destruction project to destroy old or damaged hard drives.

Your Information Security Officer or Information Technology (IT) staff should be contacted if you have any media that needs to be destroyed.



Confidentiality

Part 4 of 4

Audio:

Please ensure that information stored on paper or on a computer are properly destroyed before anything is thrown away.

Text:

Confidentiality Tips

- When possible, store information on your facility's network drives—not your desktop computer.
- If you see computers being excessed without full data erasure, let your ISO know.
- Understand the concept that clicking on the **Delete** button doesn't really delete a file completely from your computer.
- Follow your local policies and procedures for disposing of printed copies containing sensitive information by contacting your ISO for media destruction procedures. These documents should be shredded using an NSA approved cross-cut shredder. More information on the destruction of paper records can be found in [VA Directive 6371, Destruction of Temporary Paper Records](#).



Ethics

Audio:

Ethics is about what is right and what is wrong. This goes beyond legal obligations and deals with actions that affect other people.

Text:

Ethics

Ethics deals with what is right and wrong. Within VA, ethics needs to be focused on providing the best health care, benefits, and services for our nations' veterans. Applied to our computing practices, this means we need to ensure we are operating our computers in a manner that supports the VA's mission. Taking this a step further, we need to also make sure we implement appropriate computer practices and do not do anything that could introduce problems into the VA's computer network or tarnish our reputation. If a mistake is made that could affect this, it is ethical to bring this mistake to our supervisor's and ISO's attention as soon as possible to prevent the issue from causing additional harm.

A quote in the area of ethics is "Proper ethics is what we practice, so we can have peace of mind and be able to sleep at night".



Knowledge Check 1

Question 1

If you believe a security risk has occurred you should:

- A. Not do anything about it
- B. Inform your ISO
- C. Contact the news media
- D. All of the above

Question 2

If you are working with medical data and you find interesting medical information about a neighbor, you should:

- A. Obey VA's Confidentiality principles and not share the information with anyone except on a need to know basis for work related purposes
- B. Tell your other neighbors, but make sure that they promise not to tell anyone
- C. Print it out and take it home, as long as you don't share it with anyone
- D. Download the information to you personal USB flash drive

Authorized Use of Equipment

Page 1 of 5

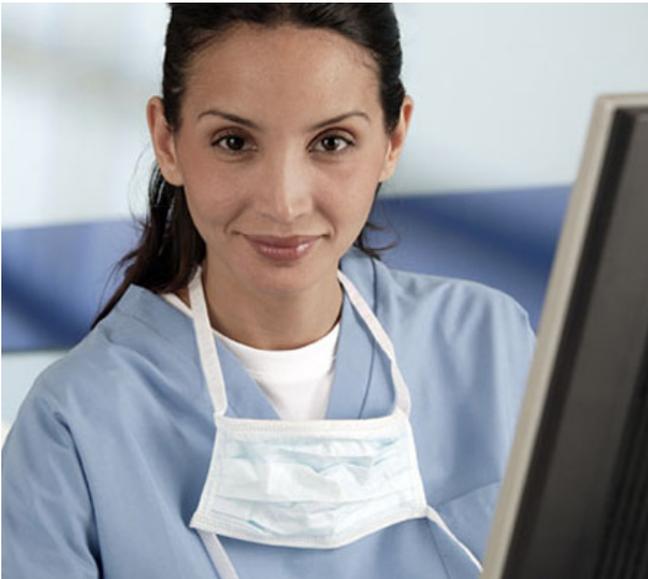
Audio:

In some situations, you may have limited personal use of certain government resources.

Text:

Authorized Use

The American people, especially our veterans, expect us to protect their information. They also expect us not to abuse or misuse the resources provided to us to accomplish our mission. As a VA employee, you may have the privilege of some "limited personal use" of certain Government resources, such as computers, email, Internet access, and telephone/fax service.



Authorized Use of Equipment

Page 2 of 5

Audio:

Some locations permit employees limited use of equipment. If this is the case at your facility, check the guidelines to make sure you do not violate what is allowed.

Text:

Limited Personal Use

This benefit is available only when it:

- Does not interfere with official VA business
- Is performed on the employee's "non-work" time
- Involves no more than minimal expense to the Government
- Is legal and ethical

These benefits may be limited or eliminated at any time, especially if you abuse these privileges. Restrictions for personal use of resources can vary between VA facilities. To protect yourself, you should discuss your limits and responsibilities with your supervisor and ISO. More can be read about limited personal use of government equipment in [VA Directive 6001](#), Limited Personal use of Government Office Equipment Including Information Technology.



Authorized Use of Equipment

Page 3 of 5

Audio:

There are many examples of inappropriate use of government resources.

Text:

Inappropriate Use

Examples of misuse or inappropriate use are:

- Any personal use that could slow down, delay, or disrupt Government systems or equipment. These include continuous data streams, video, sound, chain letters or other large files which slow down the VA network.
- Using VA systems to get unauthorized access to other systems.
- Activities which are illegal, inappropriate, or offensive to fellow employees or the public. These include hate speech or material that ridicules others because of their race, creed, religion, color, sex, disability, national origin, or sexual orientation.



Authorized Use of Equipment

Page 4 of 5

Audio:

Here are a few more examples of inappropriate use.

Text:

Inappropriate Use More examples of misuse or inappropriate use:

- Creating, downloading, viewing, storing, copying, or transmitting sexually explicit or sexually oriented materials
- Creating, downloading, viewing, storing, copying, or transmitting materials related to gambling, illegal weapons, terrorist activities, or any other illegal or prohibited activities
- Using Government systems or equipment to make money, to get a non-government job, or do any business activity (for example, consulting for pay, sale or administration of business transactions, sale of goods or services)



Authorized Use of Equipment

Page 5 of 5

Audio:

Here are some more examples of misuse of government resources. If you have any questions about whether an action would be considered inappropriate, ask your ISO and Supervisor.

Text:

Inappropriate Use Continued

More examples of misuse or inappropriate use:

- Posting VA information to external newsgroups, bulletin boards, or other public forums without permission. This includes any use which may make someone else think the information came from a VA official (unless approval has been obtained), or uses that are at odds with the Agency's mission or position
- Any use that could cost the Government money
- Accessing, using, copying, or sending VA computer software or data, private information, or copyrighted or trademarked information without permission

Be sure to discuss your limits and responsibilities with your supervisor and ISO.



Knowledge Check 2

Question 1

Which of the following is considered inappropriate use of government resources?

- A. Running a side business
- B. Applying for a VA job during your lunch time.
- C. Gambling
- D. Visiting a news web site during a break
- E. Choice A and C
- F. Choices B and D

Email

Part 1 of 5

Audio:

Email is a great tool that we have become dependant upon to perform our jobs. However, we need to use it appropriately to protect our veterans' information and take certain precautions to reduce the risks of spreading viruses.

Text:

Email Privacy and Security

Electronic mail (email) helps us do our jobs faster, but using email also has risks.

Email isn't like a personal letter delivered to you in a sealed envelope by the post office. Instead, email is more like a postcard that gets dependably delivered, with opportunities along the way for other people to see what it says. Since email is **not private**, never use email to send VA sensitive information about veterans or employees unless it is encrypted. If a work related issue requires you to send sensitive personal Information (SPI) about a veteran or VA employee in an email message, you are required to encrypt the message (encrypt with PKI or RMS). Using PKI to encrypt a message validates that the message is authentic, keeps it confidential, and protects the message content from being altered.



Email

Part 2 of 5

Audio:

Chain letters and hoaxes are messages that waste our time and slow down VA's network. Don't participate in forwarding either of these to other computer users.

Text:

Chain Letters and Hoaxes

Chain letters and hoax messages slow down VA's network. This type of email clogs up the network and may contain dangerous code. **NEVER** forward or reply to these messages. **DELETE** them, preferably without opening them. If you accidentally open the email, close it and delete it. **NEVER** open any attachments that come from an unknown source. Also, never reply by saying, "Please stop" it slows down VA 's email system.



Email

Part 3 of 5

Audio:

Safe email practices go a long way to prevent information security issues from arising. The old adage of "An ounce of prevention is worth a pound of cure" has proven to be very true in the information security world.

Text:

Email Hints

Here are a few tips on using email safely:

- Use virus protection software, and keep it up to date.
- Make sure your virus protection program scans all emails and attachments you send or receive.
- Learn to recognize the signs of a virus infection.
- Always be cautious when opening email from people you don't know.
- Additionally, since most computer viruses are spread by email, do not open email attachments that are from people you do not know.
- Never open emails with inappropriate subject lines.



Email

Part 4 of 5

Audio:

Here are a few more email hints which could help you to protect your VA.

Text:

More Email Hints

- Use "Reply to All" sparingly. Does everyone in your large email group really need to see your response? Often, it's more appropriate to limit your response to just the sender.
- Replying to unsolicited spam e-mail is actually more likely to increase the number of messages sent to your address. When spammers receive a reply, the reply tells them your e-mail address is valid.
- Don't forward or create hoaxes or ask people to modify their computer systems.
- Don't spread rumors using e-mail. Be suspicious of any message that tells you to forward it to others.



Email

Part 5 of 5

Audio:

Always remember that email is not a private communication tool.

Text:

More Email Hints

- Don't participate in "mail-storms". You don't need to send a message saying "me too" or "thanks" or even "please stop".
- Don't open attachments from senders you don't know.
- Don't expect privacy when using email to transmit, store, and communicate information.

If you have any questions about how to deal with spam or how to encrypt a message, talk to your ISO.



Knowledge Check 3

Question 1

What should you do if you receive an email attachment from someone you don't know?

- A. Open the attachment if the subject line seems harmless.
- B. Reply to the email and ask for more information.
- C. Do not open the attachment.
- D. Open the attachment if your virus software doesn't tell you not to.

Remote Access

Audio:

Remote access provides users that are traveling with the ability to work while they are on the road. If you use remote access, make sure that you follow VA policies to ensure that VA's sensitive information is protected. Safety in this area includes obtaining permission from your supervisor and ISO before connecting remotely, not sharing VA information or passwords, and not removing VA sensitive information from VA's protected environment without your supervisor and ISO's permission.

Text:

You are only allowed to access, use, or send VA sensitive information while off-site if you have the permission of your supervisor. Also, you can only do so when the following security steps have been taken:

You can only access, use, or send VA information from a VA-owned laptop, handheld computer, or storage device unless you have a waiver from the CIO. You must have your supervisor's permission to obtain remote access.

You must apply for this permission through your ISO.

You must have your supervisor's permission to transport, transmit, access, and use VA sensitive information outside of VA facilities.

You cannot share VA information with anyone else.

You must not share your username or password—or instructions on how to access the VA network—with anyone else.



Removable Storage Media

1 of 2

Audio:

Removable storage media may be convenient, but in order to use it certain security requirements must be followed. All removable storage devices that connect to VA's resources via USB ports (thumb drives, external ports, etc.) must be encrypted with FIPS 140-2 approved encryption.

Text:

In order to store VA sensitive information on removable storage media, you must have permission from your supervisor and your ISO. Only VA approved and procured thumb drives are allowed within VA. VA sensitive information outside of VA's protected environment must be encrypted.



Removable Storage Media

2 of 2

Audio:

If you require a USB drive to complete your job, you will need to obtain written permission from your supervisor and your ISO.

Text:

Thumb Drives

VA Handbook 6500 requires written permission from both your supervisor and designated Information Security Officer (ISO) to obtain a thumb drive.

Graphic:

Removable002.jpg



Knowledge Check 4

Question 1

Which of the following are appropriate security steps when working remotely?

- A. Not sharing VA data with anyone outside of the VA
- B. Obtaining your supervisors permission
- C. Not sharing your username and password
- D. Not storing VA sensitive data on your system without appropriate approvals and encryption.
- E. All of the above

Malware

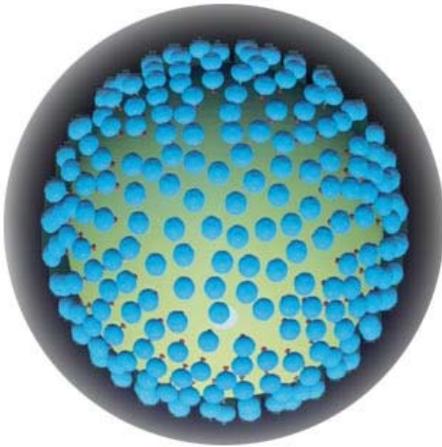
Page 1 of 7

Audio:

Malware are dangerous programs, written with malicious intentions to either do harm or steal information. Viruses are one of many different malware programs that could infect your computer equipment.

Text:

High-tech vandals have created dangerous programs that infect computer systems. These programs vary in how they infect and damage systems and are collectively called "Malware". When our systems become infected with malware they may not operate properly.



Malware

Page 2 of 7

Audio:

Worms are malware viruses that replicate over and over again. The intention of a worm is to tie up computer and network resources so that users will have a difficult time working and communicating. Worms have had a history of causing problems and worms such as Code Red caused the Internet to slow down on a global basis.

Text:

Viruses

Viruses are one type of malware that attack computers. Viruses find their way into computers by attaching themselves to files that are downloaded or transferred between computers. They can be spread many ways—from a CD, DVD, removable storage devices, web site, or email. It takes time and money to defend against viruses.

Worms

Worms infect systems and then replicate themselves. They are a simple virus that can make a copy of itself over and over again. A worm can be dangerous because it quickly uses all of the available memory on your system and brings it to a halt. Viruses that can get around VA protections and attack one computer after another are even more dangerous.

Malicious email

Malicious email hoaxes are not viruses but they can still be dangerous. In most cases, the sender asks you to forward a warning message to everyone you know. A good example of an email hoax is one that has a subject line saying, "Delete this file immediately". The message tells you how to locate a computer file and delete it. A hoax may offer a way to help you fix a problem, but when you do what it asks, it actually disables your system.

Even harmless messages, can still cause problems. Harmless messages forwarded to many other people slow down the VA network, which also slows down the process of serving America's veterans.

Trojan Horses

Another type of virus is a Trojan horse. The term "Trojan horse" comes from a story in Homer's Iliad. The ancient Greeks gave a giant wooden horse to their enemies, the Trojans, as a peace offering. After the horse was moved inside Troy's city walls, Greek soldiers came out of the horse's empty belly and opened the city gates. This allowed more soldiers to enter Troy and destroy it.

These programs may seem harmless. Even though they do not replicate themselves, they can be just as destructive as viruses and worms. Their mission is to get destructive viruses into computers and networks.

Malware

Page 3 of 7

Audio:

Your computers have antiviral software installed on them. This software is maintained by your computer administrators.

Text:

Antivirus Software

VA uses a Department-wide antivirus program. Antivirus software is automatically installed and updated. However, new viruses are developed every day. They can be spread from inside or outside VA. There is no protection from newly discovered viruses. That's why it is important for you to protect yourself and the VA.



Malware

Page 4 of 7

Audio:

Odd computer behavior can be a sign of malware.

Text:

Symptoms

There may be a problem if your computer has any of these symptoms:

- Reacts slower than usual
- Stops running for no apparent reason
- Fails to start ("boot")
- Seems to be missing important files
- Prevents you from saving your work



Malware

Page 5 of 7

Audio:

Here are a few tips to help you deal with malware. As with most information security practices, prevention goes a long way.

Text:

Malware Tips

Here are a few tips:

- Delete email messages from unknown senders or messages with unusual subject lines, such as "Open this immediately".
- Never stop or disable your antiviral program.
- Make sure your files are backed up on a regular schedule. Check with your IT staff to ensure your information is being backed up.



Malware

Page 6 of 7

Audio:

Email attachments and clicking on links inside of emails are a very prominent way in which malware can infect your system. This is why our email should not be abused.

Text:

More Malware Tips

Set your virus protection software to scan your emails and attachments.

Be very careful if someone sends you an attachment containing executable code. You can recognize these by the file extensions, such as: .exe, .vbs, .js, .jse, .wsf, .vbe, and .wsh.

Do not delete any system files when asked to do so in an e-mail; report this to your ISO.



Malware

Page 7 of 7

Audio:

Having up to date antiviral software installed on your computer is essential in protecting your system and the VA network from an infection. If you have any doubt that the antiviral software installed on your computer is up to date, contact your IT staff or ISO.

Text:

Malware Summary

All VA computers must have virus protection software. To work properly, virus protection must be kept up to date. New updates are issued nearly every day. Contact your ISO or Information Technology staff if your VA computer is not up to date. While many sites automatically update virus protection software on network computers, some systems are not updated automatically. It is critical to update your antiviral protection regularly.

To learn more about computer viruses and your role in viral defense, talk to your ISO.



Knowledge Check 5

Software specifically designed to damage, corrupt, and disrupt a computer or network is known as:

- A. My Favorites
- B. Malicious software or "malware"
- C. Junk mail
- D. Spam

Question 2

If you think your computer is infected with a virus, you should tell:

- A. Your computer manufacturer
- B. Your Information Security Officer (ISO)
- C. Acme Virus Protection, Inc.
- D. Your supervisor
- E. None of the above

Social Engineering

Page 1 of 4

Audio:

With well protected networks, hackers or crackers have a hard time breaking in using technological approaches. In these cases, they will resort to social engineering and depend on people's kindness or sense of trust to steal information or resources.

Text:

What is Social Engineering

Social engineering happens when a person tries to gain your trust in order to get information and resources which he or she can use for harm. This is an important information security issue!



Social Engineering

Page 2 of 4

Audio:

Be careful not to provide

Text:

Social Engineering Methods

A Social Engineer may try to trick you into giving them your password to illegally gain access to your system or information about VA's patients, beneficiaries and dependents, and employees. We know you want to be helpful, but social engineers may try to take advantage of your kindness.

If people ask you for VA sensitive personal information (SPI), make sure you know who they are and if they really need access to the information. Also, make sure they have permission to get such information or access it as part of their job.



Social Engineering

Page 3 of 4

Audio:

If someone asks you for something that seems unusual, contact your supervisor before proceeding. A social engineer posing as an IT specialist can gain access to a lot of resources if you give them your password.

Text:

Social Engineering Example

One example of social engineering that hurt a VA facility was a phone call from someone claiming to be from "the phone company". The thief said he was testing lines and long distance circuits. The thief then asked an employee to dial a special code, which gave him access to a long distance service. This scam resulted in thousands of dollars worth of unauthorized calls being made at VA's expense.



Social Engineering

Page 4 of 4

Audio:

None

Text:

You are the First Line of Defense

As we learn more about the tactics hackers use to get access to VA's information and computer systems, hackers continue to look for new ways to get around our protections. Social engineers will rarely ask for sensitive information directly, but will work on gaining your trust and manipulate you into assisting them in getting the information and resources.

You have to be diligent in protecting the VA from the tactics of social engineers because you are our first line of defense.



Public Peer-to-Peer File Sharing

1 of 2

Audio:

Peer-to-peer file sharing can cause major security issues within the VA and is prohibited.

Text:

Peer-To-Peer Programs

Public peer-to-peer file sharing (commonly known as "P2P") refers to programs that let anonymous files be shared between computers. There are times when using P2P is helpful. But most of the time, these programs break the law by sharing copyrighted music, videos, and games. Some common public P2P programs are Kazaa, Freewire, Grokster, and Morpheus.

Public P2P is not allowed at VA.



Public Peer-to-Peer File Sharing

2 of 2

Audio:

Please protect our computers by not using Peer-to-peer file sharing.

Text:

Peer-To-Peer Dangers

P2P programs also can be used to spread viruses and "spyware". Spyware programs track what you do on your computer and send information to thieves and hackers—without you knowing it. For example, someone could use spyware to get information about you, your coworkers, veterans, and veterans' families. This information could be used to steal your identity, buy items on a veteran's credit card, or collect personal financial information about a VA employee. In addition, P2P file-sharing makes the VA network run slower.

Don't be a victim. Use your computer wisely. If you think your computer may have P2P software or spyware, tell your ISO.



Knowledge Check 6

Question 1

Social engineering is a way for people to gain your trust so they can get you to give them information or access to VA resources they shouldn't have.

True

False



Wireless Network Security

Page 1 of 3

Audio:

Due to wireless technologies' convenience, it is being used by many federal agencies. An important item to note here is that the only time a computer is permitted to connect to the VA network wirelessly, is if the connection is encrypted using a FIPS 140-2 validated method.

Text:

Wireless Networks and The VA

If you use a wireless network, it is important you know how to use it safely and know the potential consequences if you don't. Wireless networks, which use radio waves to transmit data, are being used more often by Federal agencies. They allow users to do their work while moving around from one location to another. Poorly controlled wireless networks can allow sensitive information, passwords, and other information to be read, changed, or transmitted by unauthorized users. If a wireless local area network is set up, it needs to be encrypted using a FIPS 140-2 validated method.



Wireless Network Security

Page 2 of 3

Audio:

Improperly used wireless technologies can introduce a multitude of vulnerabilities to the VA's network. If you are using this technology be aware of the potential issues and take all necessary precautions.

Text:

Wireless Dangers

Here are some examples of the dangers associated with wireless networks:

- Another person can eavesdrop on a transmission between two workstations (e.g., a wireless PDA and a base station).
- An attacker can analyze traffic to learn more about an organization's communication patterns, such as set days or times personal information is sent from one employee to another.
- By intercepting your logon information via eavesdropping on a transmission, an attacker can pretend to be you to get access to private information, to change data, or to send it to someone else.



Wireless Network Security

Page 3 of 3

Audio:

In many cases wireless networks can assist us in completing our jobs. If you are a user of a wireless network, please take extra precautions to protect our networks.

Text:

More Wireless Dangers

- An attacker can become "the man in the middle" by intercepting messages, stopping them from being sent, or transmitting them to someone else.
- An attacker can change or delete a message.
- An attacker can jam a wireless network with extra radio signals to stop you from accessing information. Other devices such as cordless phones or microwaves can prevent a wireless network from working properly.

If you use a wireless network, contact your ISO to learn more about how you can do your work safely.



Laptop Security

Audio:

Laptops are very useful tools in today's computing world. If you use a laptop you can protect the information on it by; ensuring that the hard drive is encrypted, making sure that antiviral and other software updates are installed, and practicing physical security techniques.

Text:

Protection of data stored on laptops is a very important component in securing our veteran's' data. Laptops can contain large amounts of data that could fall into the wrong hands if proper precautions are not taken. The following list can assist in protecting the data on laptops:

- Ensure all data on the hard drive is encrypted.
- Make sure your system administrator maintains your laptop and all the latest software upgrades are installed. This includes antiviral software, personal firewalls, software patches, and Virtual Private Network (VPN).
- Physically secure your laptop. This includes keeping it close to you while traveling and using locking cables if you must leave it in a hotel room.
- Taping contact information such as a business card to the bottom of a laptop could aid in recovery, if it is lost or stolen.



Knowledge Check 7

Question

Practices that contribute to secure laptop usage include:

- A. Encrypting the hard drive
- B. Ensuring that the systems administrator is keeping the laptop updated
- C. Keeping the laptop protected while traveling
- D. All of the above



Passwords

Page 1 of 6

Audio:

Passwords are an essential part of any security program. To do your part in protecting the VA's information, you must protect your password. This means that you must have a strong password that is not shared with anyone.

Text:

Importance of Passwords

Passwords are important tools for protecting VA information and information systems and getting your job done.

They ensure that you and only you have access to the information you need. Keep your password secret.

If you have several passwords, store them in a safe and secure place that no one else knows about.



Passwords

Page 2 of 6

Audio:

Strong passwords have at least 8 characters, include upper and lower case letters, numbers, and special characters.

Text:

Strong Passwords

VA requires strong passwords on all information systems. Passwords must:

- Be changed at least every 90 days
- Have 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 @

Using these rules will provide you with a "Strong" password.



Passwords

Page 3 of 6

Audio:

When hackers or crackers attempt to break into computing systems using passwords, they begin with common everyday words. They actually use lists of dictionary words and names in automated password cracking tools. Other ways they try to crack passwords is by using birthdays, social security numbers, and addresses. To ensure that you are using strong passwords stay away from using any of these items.

Text:

Passwords Rules of Thumb

- Don't use words found in a dictionary.
- Follow the rules for strong passwords.
- Don't use personal references (names, birthdays, addresses, etc.).
- Change your passwords at least every 90 days. If you suspect someone may know your password, change it immediately and inform your ISO.
- Never let anyone stand near you while you type your password. Ask people to turn away while you type it, and don't let them see your keyboard while you type.
- If you have several passwords to remember **you may** write them down, but keep them in a locked place so no one else can get to them.



Passwords

Page 4 of 6

Audio:

Strong passwords can be developed by using parts of each word in a phrase. This in combination with numbers and special characters can help you develop a strong password that is easy for you to remember.

Text:

Remembering Passwords

Since childhood, many people have used simple rhythms to remember things. Can you remember how you learned the alphabet, months of the year, state capitols, etc.? Sometimes people use "mnemonics", which are things such as formulas or rhymes that help with memory.

Below is an example of a mnemonic used to remember the planets of our solar system:

"My Very Excellent Mother Just Served Us Nine Pizzas" This helps you remember the names and order of the planets.



Passwords

Page 5 of 6

Audio:

Mnemonics can help you develop and remember strong passwords.

Text:

Remembering Passwords

Another sample mnemonic: **M**ercury, **V**enus, **E**arth, **M**ars, **J**upiter, **S**aturn, **U**ranus, **N**eptune, **P**luto

It may sound silly but it works. A simple mnemonic just needs to make sense to you. Mnemonics are a useful tool in constructing passwords that cannot be found in a dictionary. How about using this as a password for the mnemonic above:

MVEMJS,unp

For more information about passwords, ask your ISO.



Passwords

Page 6 of 6

Audio:

As mentioned earlier, strong passwords are an essential part of any information security program. In order to do your part, do not share your password with anyone. This would compromise the VA's security and possibly cause issues for yourself.

Text:

Protecting Your Password

Your username and password protect you and the information stored on VA computers.

When you log into a VA system, the combination of your user name and password identifies YOU as the person accessing the system and information. All actions taken after you log into the system are identifiable back to you, so it is important that you **NEVER** share your log in information.

If someone else uses your account information, you are responsible. Guard your password and never disclose it to anyone!



Backups

Part 1 of 3

Audio:

Backing up your information is an essential part of protecting VA information. We must always remember that computers are mechanical equipment and that all mechanical equipment will eventually fail. Therefore the information stored on your local hard drive, also needs to be stored someplace else such as a drive mapped to a server.

Text:

Importance of Backups

Any work you do on VA's computers is important. It is important to you because of the time and effort expended to create it. It is important to VA and to veterans because it supports our mission. There are some resources we can't afford to lose, so database backups are systematically and routinely created on systems such as VistA, BDN and others. Backups are cheap insurance.



Backups

Part 2 of 3

Audio:

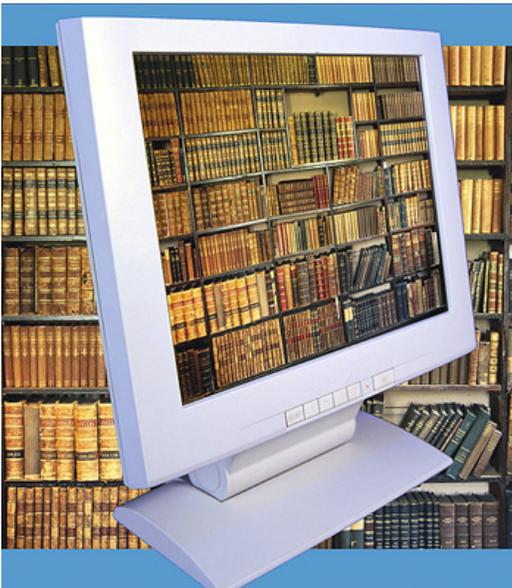
Backing up data is an important step in protecting your hard work.

Text:

Backup Routines

VA information technology staff work hard to make sure the VA data is safe and routinely backed up. Most facilities have routines that automatically backup data on users' computers to a networked server in a computer room.

The question is not **if** you will ever need to use your backup—the question is **when**; so making backups is a smart practice for your home computer, too.



Backups

Part 3 of 3

Audio:

Information that resides on your computer is very valuable and it needs to be backed up. Consider all the hard work that you have done to complete those documents. You would not want a hardware failure to ruin weeks or even months of your hard work.

Text:

Your Role for Backups

What you can do to assist in this matter is:

Keep your files in one location, such as the "My Documents" folder or a mapped network drive. This will make it easy to find and create backup files.

If you are a remote user or travel a lot, you should check with your IT staff to ensure your data is being backed up.

If you have any concerns about how your system is being backed up, contact your IT staff or ISO.



Knowledge Check 8

Question 1

Which of the following are secure password practices?

- A. Using upper case, lower case, numbers, and special characters
- B. Using words found in a dictionary
- C. Using names, birthdays or locations
- D. Using social security or license plate numbers

Question 2

Which of the following items are recommended for backing up your files?

- A. Store files in a single location such as the My Documents folder.
- B. Computers are mechanical equipment which can fail. Therefore your data should be backed up on a regular basis.
- C. If you are not sure your backups are occurring regularly, contact your IT staff.
- D. All of the above.

Incidents

Page 1 of 4

Audio:

Unfortunately information security incidents do happen. However, your response during one of these incidences can prevent it from blowing up into something out of control. For instance if a new virus that could harm all the computers in the VA hits your computer first, your prompt response could prevent a catastrophe. By notifying your IT staff and ISO of such an incident, they could take proper actions.

Text:

Dangers of Incidents

You know how important computers are when we are doing our jobs. At VA, so much of what we do depends on our computers.

Security incidents include the following:

A virus attack

A lost or stolen computer

Files are missing or were compromised

Sensitive personal information (SPI) was shared with people who do not have a need to know

All of these are examples of computer-related incidents. It is important to tell your supervisor and ISO when you see such incidents.



Possible Incidents

Page 2 of 4

Audio:

Leakage of sensitive data is one of many possible incidents.

Text:

The list below include possible incidents that could occur.

- A stranger is sitting at a VA computer, whom you believe has no authorization to be there.
- A veteran's personal medical information is left unattended on a desk, a copier, or a computer screen.
- A co-worker sends a patient's sensitive personal information (such as a combination of a full name and social security number or account number) to an outside e-mail address – even if it is the patient's personal physician – via unencrypted e-mail.
- You discover an open box with reams of computer print-outs containing sensitive personal information standing unattended by a dumpster.



Incidents

Page 3 of 4

Audio:

If you think a information security incident has occurred, you should gather information about what happened and report it to your ISO and supervisor immediately. This should be done by calling them or reporting it in person. It is not your duty to report this to the press or other individuals outside of the VA.

Text:

Incident Do's and Don'ts

If you think a security incident has occurred, you should:

- Write down the date, time, and location the incident took place as well as the computers which may have been affected.
- Tell your ISO and Privacy Officer what happened.
- Write down any error messages that showed up on your computer screen.
- Write down any Web addresses, server names, or IP addresses involved in the incident.

Protect yourself. If you witness what you believe to be a security or privacy incident, you are obligated to report it immediately to your facility/office ISO, Privacy Officer (PO) and/or supervisor. If you fail to report such an action, you may be considered an accomplice to that action.



Incidents

Page 3 of 3

Audio:

Loss or theft of portable equipment has significantly grown and is a major cause of security breaches. These data breaches violates our promise to our Veterans and put them at risk for identify theft.

Text:

Incident Do's and Don'ts

You've probably heard about the theft of electronic information from a VA employee's home. The data included names, addresses and social security numbers of millions of veterans. Fortunately, the information was recovered and was never accessed.

So, when you suspect an incident may have occurred, it's very important you tell your ISO, Privacy Officer and supervisor immediately (i.e. one hour or less). Don't wait.

It's best to contact your ISO/PO in person or by telephone rather than by email. You may **not** contact the media (radio, TV, newspapers) or anyone outside your VA facility. If a crime is involved, (such as an item was stolen) you also need to report it to VA law enforcement. VA Handbook 6500.2, Managing Security and Privacy Incidents, provides additional procedure on incident management.



Rules of Behavior

1 of 2

Audio:

The VA National Rules of Behavior you sign in order to access VA information and information systems clearly states your information security responsibilities.

Text:

What are the VA National Rules of Behavior:

Everyone who accesses VA's information and information systems must understand their security roles and responsibilities.

Information security do's and don'ts are established in a document known as " VA's National Rules of Behavior".

Prior to being granted access to VA's information and information systems, users must agree to the VA National Rules of Behavior, stating they have read, understand, and will abide by these security rules.

The VA National Rules of Behavior must be read and signed each year.

The VA National Rules of Behavior also contains the consequences of inappropriate behavior.

Consequences may range from a written reprimand to losing your job, depending upon the violation.



Rules of Behavior

2 of 2

Audio:

Rules of Behavior ensure everyone is aware of their security responsibilities and helps to protect our veterans' data

Text:

More on VA's National Rules of Behavior:

- Rules of Behavior ensure everyone is aware of their security responsibilities and helps to protect our veterans' data.
- ISOs are available to explain and provide clarification to anyone who needs assistance understanding ROB.
- Additionally, VA employees are responsible for protecting Personally Identifiable information. VA Directive 6600, Responsibility of Employees and Others supporting VA. In Protecting Personally Identifiable Information (SPI), requires all employees to treat sensitive information of others the same as they would like theirs treated.
- A computer based training (CBT) module is available for users explaining the VA's National Rules of Behavior – contact your ISO for more information.

[Read VA Directive 6600](#)



VA National Rules of Behavior

1 of 2

Audio:

The next screen will take you to the **VA National Rules of Behavior**. Please read, acknowledge, and accept the Rules of Behavior.

Text:

The last pages in this course will provide you with the **VA National Rules of Behavior**. You will need to print and sign the Rules of Behavior in order to be able to receive credit for completion of this course. Provide a signed copy of the Rules of Behavior to your supervisor and make a copy for yourself.

These rules serve to provide notice of what is considered acceptable use of all VA information and information systems, VA sensitive information, and behavior of VA users.

Final Summary

1 of 2

Audio:

The VA and our nation's veterans are depending on you to do your part in information security protection. Keep in mind that our information and information systems also assist with our readiness during national emergencies. Your safe practices can protect VA information and contribute greatly toward providing our Veterans with top quality services. This will benefit you, the Veteran, the VA, and our nation. Thank you for doing a great job in this area.

Text:

VA's information and information systems are a major part of how we help veterans. They also affect our readiness to work with other Federal agencies, such as the Departments of Defense, Health and Human Services, and Homeland Security, during national emergencies.

The FBI has warned all Federal agencies that their systems, and the information in those systems, are potential targets for attacks. Now more than ever, VA's systems and the information they contain must be available to serve our Nation and its veterans. Please be careful. Don't do anything that might damage our information and information systems.



Final Summary

2 of 2

Text:

The work we do at VA is an important part of our Nation's security and this puts VA's information systems at risk. VA employees must do their part to prevent attacks that would breach the security of the systems and the information that could interrupt care of our veterans. You have just learned some important information that will assist you with guarding information and what steps to take if a breach occurs.

Remember, if an incident occurs report it to your ISO and PO immediately. If your ISO is not available, contact your Network ISO.



Knowledge Check 9

Question 1

If you think a computer security incident has occurred, you should:

1. Ask your friend down the hall what to do.
2. Gather all the information you can, and report it to your ISO and PO.
3. Contact your local media.
4. All of the above.

Question 2

Which of the following are rule violations that should be reported?

1. A co-worker sends a patient's sensitive personal information to the patient's physician outside email address via an unencrypted email.
2. A stranger who you believe has no authorization to be there is sitting at a VA computer.
3. A veteran's personal medical information is left on a desk, copier or computer screen where unauthorized individuals can see it.
4. All of the above.

Reference Page

VA Directives

[VA Directive and Handbook 6500, Information Security Program](#)

[VA Directive 6300, Records Information Management](#)

[VA Directive 6301, Electronic Mail Records](#)

[VA Directive and Handbook 0710, Personnel and National Information Security –](#)

[VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology](#)

[VA Directive 6502, VA Enterprise Privacy Program](#)

[VA Directive 6371, Destruction of Temporary Paper Records](#)

[VA Handbook 6500.2, Managing Security and Privacy Incidents](#)

Federal Policies

[Federal Information Security Management Act \(FISMA\) Title III, 2002 E-Gov Act](#)

[OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources](#)

[Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#)

[Clinger-Cohen Act of 1996](#)

[OMB Memorandum M-06-16, Protection of Sensitive Agency Information](#)

[OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management \(July 17, 2006\)](#)

[NIST Special Publications – Computer Security Resource Center – CSD – 800 Series](#)

[Privacy Act of 1974 \(5 USC 552a\)](#)

Department of Veterans Affairs (VA) National Rules of Behavior

1. Background

a. Section 5723(b)(12) of title 38, United States Code, requires the Assistant Secretary for Information and Technology to establish “VA National Rules of Behavior for appropriate use and protection of the information which is used to support Department’s missions and functions.” The Office of Management and Budget (OMB) Circular A-130, Appendix III, paragraph 3(a)(2)(a) requires that all Federal agencies promulgate rules of behavior that “clearly delineate responsibilities and expected behavior of all individuals with access” to the agencies’ information and information systems, as well as state clearly the “consequences of behavior not consistent” with the rules of behavior. **The National Rules of Behavior that begin on page G-3, are required to be used throughout the VA.**

b. Congress and OMB require the promulgation of national rules of behavior for two reasons. First, Congress and OMB recognize that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the VA data that it contains or that may be accessed through it, as well as the security and protection of VA information in any form (e.g. digital, paper), are essential aspects of their job. Second, individuals must be held accountable for their use of VA information and information systems.

c. VA must achieve the Gold Standard in data security which requires that VA information and information system users protect VA information and information systems, especially the personal data of veterans, their family members, and employees. Users must maintain a heightened and constant awareness of their responsibilities regarding the protection of VA information. The Golden Rule with respect to this aspect of an employee’s job is to treat the personal information of others the same as they would their own.

d. Since written guidance cannot cover every contingency, personnel are asked to go beyond the stated rules, using “due diligence” and highest ethical standards to guide their actions. Personnel must understand that these rules are based on Federal laws, regulations, and VA Directives.

2. Coverage

a. The attached VA National Rules of Behavior must be signed annually by all VA employees who are provided access to VA information or VA information systems. The term VA employees includes all individuals who are employees under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and other trainees. Directions for signing the rules of behavior by other individuals who have access to VA information or information systems, such as contractor employees, will be addressed in subsequent policy. VA employees must initial and date each page of the copy of the VA National Rules of Behavior; they must also provide the information requested on the last page, sign and date it.

b. The VA National Rules of Behavior address notice and consent issues identified by the Department of Justice and other sources. It also serves to clarify the roles of management and system administrators, and serves to provide notice of what is considered acceptable use of all VA information and information systems, VA sensitive information, and behavior of VA users.

c. The VA National Rules of Behavior use the phrase “VA sensitive information”. This phrase is defined in VA Directive 6500, paragraph 5q. This definition covers all information as defined in 38 USC 5727(19), and in 38 USC 5727(23). The phrase “VA sensitive information” as used in the attached VA National Rules of Behavior means:

All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the

ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information, financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information, information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege, and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

d. The phrase "VA sensitive information" includes information entrusted to the Department.

3. Rules of Behavior

a. Immediately following this section is the VA approved National Rules of Behavior that all employees (as discussed in paragraph 2a of Appendix G) who are provided access to VA information and VA information systems are required to sign in order to obtain access to VA information and information systems.

Department of Veterans Affairs (VA) National Rules of Behavior

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including VA sensitive information, or information systems of the U.S. Department of Veterans Affairs.

1. GENERAL RULES OF BEHAVIOR

A. I understand that when I use any Government information system, I have NO expectation of Privacy in VA records that I create or in my activities while accessing or using such information system.

B. I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. Authorized VA personnel include my supervisory chain of command as well as VA system administrators and Information Security Officers (ISOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (OIG), VA, and law enforcement personnel.

C. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting information on VA systems, modifying VA systems, unauthorized denying or granting access to VA systems, using VA resources for unauthorized use on VA systems, or otherwise misusing VA systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.

D. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal, civil, and/or administrative penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include: suspension of access privileges, reprimand, suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

E. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my Operating Unit's Information Security Officer (ISO), Privacy Officer (PO), and my supervisor as appropriate.

F. I understand that I have a duty to report information about actual or possible criminal violations involving VA programs, operations, facilities, contracts or information systems to my supervisor, any management official or directly to the OIG, including reporting to the OIG Hotline. I also understand that I have a duty to

immediately report to the OIG any possible criminal matters involving felonies, including crimes involving information systems.

G. I understand that the VA National Rules of Behavior do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

H. I understand that the VA National Rules of Behavior do not supersede any local policies that provide higher levels of protection to VA's information or information systems. The VA National Rules of Behavior provide the minimal rules with which individual users must comply.

I. I understand that if I refuse to sign this VA National Rules of Behavior as required by VA policy, I will be denied access to VA information and information systems. Any refusal to sign the VA National Rules of Behavior may have an adverse impact on my employment with the Department.

2. SPECIFIC RULES OF BEHAVIOR.

a. I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor and the ISO when the access is no longer needed.

b. I will follow established VA information security and privacy policies and procedures.

c. I will use only devices, systems, software, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware or public domain.

d. I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties except as provided for in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. I also agree that I will not engage in any activities prohibited as stated in section 2c of VA Directive 6001.

e. I will secure VA sensitive information **in all areas** (at work and remotely) and in any form (e.g. digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all VA sensitive information must be in a protected environment at all times or it must be encrypted (using FIPS 140-2 approved encryption). If clarification is needed whether or not an environment is adequately protected, I will follow the guidance of the local Chief Information Officer (CIO).

f. I will properly dispose of VA sensitive information, either in hardcopy, softcopy or electronic format, in accordance with VA policy and procedures.

g. I will not attempt to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff.

h. I will not attempt to alter the security configuration of government equipment unless authorized. This includes operational, technical, or management security controls.

i. I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the VA minimum requirements for the systems that I am authorized to use and are contained in Appendix F of VA Handbook 6500.

j. I will not store any passwords/verify codes in any type of script file or cache on VA systems.

k. I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.

l. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any VA electronic communication system.

m. I will not auto-forward e-mail messages to addresses outside the VA network.

n. I will comply with any directions from my supervisors, VA system administrators and information security officers concerning my access to, and use of, VA information and information systems or matters covered by these Rules.

o. I will ensure that any devices that I use to transmit, access, and store VA sensitive information outside of a VA protected environment will use FIPS 140-2 approved encryption (the translation of data into a form that is unintelligible without a deciphering mechanism). This includes laptops, thumb drives, and other removable storage devices and storage media (CDs, DVDs, etc.).

p. I will obtain the approval of appropriate management officials before releasing VA information for public dissemination.,

q. I will not host, set up, administer, or operate any type of Internet server on any VA network or attempt to connect any personal equipment to a VA network unless explicitly authorized **in writing** by my local CIO and I will ensure that all such activity is in compliance with Federal and VA policies.

r. I will not attempt to probe computer systems to exploit system controls or access VA sensitive data for any reason other than in the performance of official duties. Authorized penetration testing must be approved in writing by the VA CIO.

s. I will protect Government property from theft, loss, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for VA activities.

t. I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by the VA on VA equipment or on computer systems that are connected to any VA network.

u. If authorized, by waiver, to use my own personal equipment, I must use VA approved virus protection software, anti-spyware, and firewall/intrusion detection software and ensure the software is configured to meet VA configuration requirements. My local CIO will confirm that the system meets VA configuration requirements prior to connection to VA's network.

v. I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee at the time of system problems.

w. I will not disable or degrade software programs used by the VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or to create, store or use VA information.

x. I agree to allow examination by authorized OI&T personnel of any personal IT device [Other Equipment (OE)] that I have been granted permission to use, whether remotely or in any setting to access VA information or information systems or to create, store or use VA information.

y. I agree to have all equipment scanned by the appropriate facility IT Operations Service prior to connecting to the VA network if the equipment has not been connected to the VA network for a period of more than three weeks.

z. I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

aa. I understand that if I must sign a non-VA entity's Rules of Behavior to obtain access to information or information systems controlled by that non-VA entity, I still must comply with my responsibilities under the VA

National Rules of Behavior when accessing or using VA information or information systems. However, those Rules of Behavior apply to my access to or use of the non-VA entity's information and information systems as a VA user.

bb. I understand that remote access is allowed from other Federal government computers and systems to VA information systems, subject to the terms of VA and the host Federal agency's policies.

cc. I agree that I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA-approved remote access software and services. I must use VA-provided IT equipment for remote access when possible. I may be permitted to use non-VA IT equipment [Other Equipment (OE)] only if a VA-CIO-approved waiver has been issued and the equipment is configured to follow all VA security policies and requirements. I agree that VA OI&T officials may examine such devices, including an OE device operating under an approved waiver, at any time for proper configuration and unauthorized storage of VA sensitive information.

dd. I agree that I will not have both a VA network connection and any kind of non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my local CIO.

ee. I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA's CIO. I agree that I will not access, transmit or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

ff. I will obtain my VA supervisor's authorization, in writing, prior to transporting, transmitting, accessing, and using VA sensitive information outside of VA's protected environment..

gg. I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access VA sensitive information or information systems are adequately secured in remote locations, e.g., at home and during travel, and agree to periodic VA inspections of the devices, systems or software from which I conduct access from remote locations. I agree that if I work from a remote location pursuant to an approved telework agreement with VA sensitive information that authorized OI&T personnel may periodically inspect the remote location for compliance with required security requirements.

hh. I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the VA to protect sensitive data.

ii. I will not store or transport any VA sensitive information on any portable storage media or device unless it is encrypted using VA approved encryption.

jj. I will use VA-provided encryption to encrypt any e-mail, including attachments to the e-mail, that contains VA sensitive information before sending the e-mail. I will not send any e-mail that contains VA sensitive information in an unencrypted form. VA sensitive information includes personally identifiable information and protected health information.

kk. I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific VA systems. I understand that those specific rules of behavior may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

3. Acknowledgement and Acceptance

a. I acknowledge that I have received a copy of these Rules of Behavior.

b. I understand, accept and agree to comply with all terms and conditions of these Rules of Behavior.

[Print or type your full name] Signature

Date

Office Phone Position Title