

**Information Systems Security Awareness (v5)  
Security Tips Summary**

**A Risk to One is a Risk to All!**

Remember to:	By following these tips:
<b>Create Secure Passwords</b>	<ul style="list-style-type: none"> <li>• Do not use personal information</li> <li>• Do not use common phrases or words</li> <li>• Longer passwords are more secure</li> <li>• Change password according to your organization's policy</li> <li>• Combine letters, numbers, special characters</li> <li>• Use different passwords for work, home, and general websites</li> <li>• Do not write down your password, memorize it</li> </ul>
<b>Avoid Phishing Attempts</b>	<ul style="list-style-type: none"> <li>• Do not access the web by selecting links in e-mails or pop-up messages</li> <li>• Contact the organization using a telephone number</li> <li>• Delete the e-mail</li> <li>• View all e-mail in the plain text</li> <li>• Type the web address or use bookmark</li> <li>• Report e-mails requesting personal information to your POC</li> <li>• Use caution when visiting sites with expired certificates</li> <li>• Report trusted sites with expired certificates</li> </ul>
<b>Avoid Spear Phishing Attempts</b>	<ul style="list-style-type: none"> <li>• Assume all unsolicited information requests are phishing attempts</li> <li>• Never reveal any personal information in an e-mail</li> <li>• Look for digital signatures</li> <li>• Never give out your password; IT will never ask for your password</li> <li>• Never reveal any personal information in an e-mail</li> </ul>
<b>Avoid Whaling Attempts</b>	<ul style="list-style-type: none"> <li>• Contact sender by other means before opening a doubtful attachment or clicking on a link</li> <li>• Never give out organizational, personal, or financial information to anyone by e-mail</li> <li>• Follow your organization's IT security policies and guidelines</li> <li>• Contact your security POC regarding suspected whaling attempts</li> </ul>
<b>Forward E-mails Carefully</b>	<ul style="list-style-type: none"> <li>• Use online sites to confirm or expose potential e-mail hoaxes</li> <li>• Do not forward e-mail hoaxes</li> </ul>
<b>Read E-mails Carefully</b>	<ul style="list-style-type: none"> <li>• View e-mail in plain text</li> <li>• Disable preview panes in Outlook</li> <li>• Use caution when opening e-mail</li> <li>• Scan all attachments</li> <li>• Delete e-mail from senders you do not know</li> <li>• Turn off automatic downloading</li> </ul>
<b>Use E-mail Appropriately</b>	<ul style="list-style-type: none"> <li>• E-mail must not:               <ul style="list-style-type: none"> <li>◦ Adversely affect performance</li> <li>◦ Reflect poorly on the Government</li> </ul> </li> <li>• Do not use e-mail to:               <ul style="list-style-type: none"> <li>◦ Sell anything</li> <li>◦ Send chain letters</li> <li>◦ Send offensive letters</li> </ul> </li> <li>• Do not send:               <ul style="list-style-type: none"> <li>◦ Mass e-mails</li> <li>◦ Jokes or Pictures</li> <li>◦ Inspirational stories</li> </ul> </li> <li>• Avoid using <i>Reply All</i></li> <li>• Personal e-mail use may be authorized</li> </ul>

**Information Systems Security Awareness (v4)**  
**Security Tips Summary (cont'd)**

Remember to:	By following these tips:
<b>Avoid Computer Misuse</b>	<p>Examples of Computer Misuse:</p> <ul style="list-style-type: none"> <li>• Viewing/downloading pornography</li> <li>• Gambling on the Internet</li> <li>• Private business/money-making ventures</li> <li>• Loading personal/unauthorized software</li> <li>• Unauthorized configuration changes</li> </ul>
<b>Protect Against Spillage</b>	<ul style="list-style-type: none"> <li>• Check all documents for sensitivity level</li> <li>• Label all files, removable media, and subject headers</li> <li>• If a spillage occurs, notify your security POC</li> <li>• When storing or transmitting sensitive information, including PII: <ul style="list-style-type: none"> <li>◦ Encrypt before storing on mobile devices or transmitting</li> <li>◦ E-mail with caution</li> <li>◦ Store on authorized system</li> <li>◦ Never transmit, store, or process on a non-sensitive system</li> </ul> </li> </ul>
<b>Avoid Social Engineering Attempts</b>	<ul style="list-style-type: none"> <li>• Do not participate in unapproved surveys on the telephone or online</li> <li>• Do not give out personal information</li> <li>• Do not give out computer or network information</li> <li>• Do not follow instructions from unverified personnel</li> <li>• Document interaction: <ul style="list-style-type: none"> <li>◦ Verify the identity of all individuals</li> <li>◦ Write down phone number</li> <li>◦ Take detailed notes</li> </ul> </li> <li>• Contact your security POC</li> </ul>
<b>Follow Physical Security Procedures</b>	<ul style="list-style-type: none"> <li>• Use ONLY your own security badge or key code</li> <li>• Never grant access for someone else</li> <li>• Maintain possession of your security badge at all times (provides access to buildings and computer systems and contains information about you that is used to verify your identity)</li> <li>• Challenge people without proper badges</li> <li>• Challenge people without proper badges</li> <li>• Be wary when people with visitor's badges ask about other people's office locations</li> <li>• Report suspicious activity</li> </ul>
<b>Avoid Computer Viruses</b>	<ul style="list-style-type: none"> <li>• Scan all external files before uploading to your computer</li> <li>• Do not e-mail an infected file to anyone</li> <li>• Contact your help desk for assistance</li> </ul>
<b>Conduct E-Commerce Cautiously</b>	<ul style="list-style-type: none"> <li>• Set your browser preferences to prompt you each time a website wants to store a cookie</li> <li>• Only accept cookies from reputable, trusted websites.</li> <li>• Confirm that site uses encrypted links (https) in URL name or web address</li> </ul>
<b>Follow FAX Procedures</b>	<ul style="list-style-type: none"> <li>• Ensure that the recipient is at the receiving end</li> <li>• Use the correct cover sheet</li> <li>• Contact the recipient to confirm receipt</li> <li>• Never transmit sensitive information via an unsecured fax machine</li> </ul>

**Information Systems Security Awareness (v4)**  
**Security Tips Summary (cont'd)**

Remember to:	Follow these tips:
<b>Follow Telework Guidelines</b>	<ul style="list-style-type: none"> <li>• You may telework from a telework center</li> <li>• You may work at home, in a dedicated work area</li> <li>• You must use authorized equipment and software</li> <li>• You must implement appropriate security measures</li> <li>• You must sign a telework agreement</li> <li>• You must sign a safety checklist</li> <li>• You must protect your data</li> </ul>
<b>Follow Travel Tips</b>	<ul style="list-style-type: none"> <li>• Be careful of information visible on your laptop</li> <li>• Ensure that the wireless security features are properly configured</li> <li>• Wireless technology (e.g., Bluetooth) is not a secure technology</li> <li>• Avoid using Government-furnished or authorized computers in non-secure environments (e.g., hotels)</li> <li>• Be caution when establishing VPN connection through non-secure environment (e.g., hotel)</li> <li>• Turn off/disable wireless capability when connected via LAN cable</li> <li>• Turn off/disable wireless capability when not in use</li> <li>• Never discuss sensitive information on an unsecured phone</li> <li>• Never discuss sensitive information on an unsecured phone</li> <li>• Maintain possession of your laptop at all times</li> <li>• Password protect and encrypt your laptop using whole disk encryption</li> <li>• Encrypt all sensitive and non-sensitive information not cleared for public release</li> <li>• Sign for and protect government furnished equipment (GFE) from loss and theft</li> <li>• Report a loss of GFE immediately to your security POC.</li> </ul>
<b>Protect Your Identity</b>	<ul style="list-style-type: none"> <li>• Ask how information will be used before giving it out</li> <li>• Pay attention to credit card and bank statements</li> <li>• Avoid common names/dates for passwords and PINs</li> <li>• Pick up mail promptly</li> <li>• Shred personal documents</li> <li>• Carry your SSN card and passport only when necessary</li> <li>• Order credit report annually</li> </ul> <p><b>How to respond to identity theft:</b></p> <ul style="list-style-type: none"> <li>• Contact credit reporting agencies</li> <li>• Contact financial institutions/creditors to place an alert on: <ul style="list-style-type: none"> <li>o Credit cards</li> <li>o Bank accounts</li> </ul> </li> <li>• Monitor credit card statements for unauthorized purchases</li> <li>• Report crime to the local police</li> </ul>
<b>Handle Removable Media Appropriately</b>	<p>Examples: thumb drives, flash drives, CDs, DVDs, external hard drives.</p> <ul style="list-style-type: none"> <li>• Encrypt all data stored on removable media</li> <li>• Encrypt in accordance with the data's classification or sensitivity level</li> <li>• Label to reflect the sensitivity level</li> <li>• Store in GSA approved storage containers at the appropriate level of classification</li> <li>• Purge all removable media before discarding</li> <li>• Follow your organization's policy for purging or discarding removable media</li> <li>• Contact your security POC for more information</li> </ul>

## Information Systems Security Awareness (v4) Security Tips Summary (cont'd)

Remember to:	Follow these tips:
<b>Handle Mobile Computing Devices Appropriately</b>	<p>Examples: Smartphones, laptops, cell phones, and other portable electronic devices (PEDs), wireless readers (e.g., Kindle and iPads); music players such as iPods).</p> <ul style="list-style-type: none"> <li>• Be extra vigilant when storing data on mobile computing devices</li> <li>• All mobile computing devices must comply with Federal policy</li> <li>• Password protect Government-issued mobile computing devices</li> <li>• Do not connect personally owned mobile computing devices to Government computers or networks</li> <li>• The Government classifies laptop computers as mobile computing devices</li> <li>• Lock your laptop screen when left unattended</li> <li>• Encrypt all sensitive and non-sensitive data not cleared for public release</li> <li>• Encrypt all Personally Identifiable Information* (PII) on mobile computing devices               <ul style="list-style-type: none"> <li>o Social Security numbers</li> <li>o Dates and places of birth</li> <li>o Mothers' maiden names</li> <li>o Biometric records</li> </ul> </li> <li>• If lost or stolen, immediately report the loss to your security POC               <ul style="list-style-type: none"> <li>o If the device contains PII, you must report the loss <b>immediately</b> to your organization's security POC or help desk</li> </ul> </li> <li>• Contact your security POC for more information</li> </ul> <p>*Note: PII is Any information about an individual maintained by an agency, including, but not limited to education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information that is linked or linkable to an individual.</p>
<b>Follow Tips for Active X and Other Mobile Code Technology</b>	<ul style="list-style-type: none"> <li>• Require confirmation before enabling</li> <li>• Only allow mobile code to run from Government trusted sites</li> </ul>
<b>Identify and Handle Sensitive Information Properly</b>	<p><b>Consult these examples to easily identify sensitive information:</b></p> <ul style="list-style-type: none"> <li>• Information that cannot be posted on a wall or on a public or internal website, for example:           <ul style="list-style-type: none"> <li>o Credit card numbers</li> <li>o Social Security Numbers</li> <li>o Employee's home telephone numbers</li> </ul> </li> <li>• Information that can originate from only specific individuals, for example:           <ul style="list-style-type: none"> <li>o Prescriptions</li> <li>o Checks</li> </ul> </li> </ul> <p><b>Handle and store properly:</b></p> <ul style="list-style-type: none"> <li>• Reduce risk of access during working hours</li> <li>• Store properly after working hours:           <ul style="list-style-type: none"> <li>o If security is present, locked or unlocked containers, desks, cabinets</li> <li>o If no security is present, locked containers, desks, cabinets</li> </ul> </li> </ul>
<b>If Permitted by Agency to Access Web Mail, Use with Caution</b>	<ul style="list-style-type: none"> <li>• Use caution if you are allowed to use web mail on Government computers.</li> <li>• By using web mail, you are bypassing firewalls and other security measures, and exposing you and your agency to potential viruses and other malware.</li> </ul>

**Information Systems Security Awareness (v4)**  
**Security Tips Summary (cont'd)**

Remember to:	Follow these tips:
<b>If Permitted by Agency to Use Social Networking Sites, Follow Best Practices</b>	<p>Use caution if you are allowed to use social networking sites on Government computers. Best practices include:</p> <ul style="list-style-type: none"> <li>• Consider carefully the information you post online about yourself and your family</li> <li>• Remember that sites own posted content</li> <li>• Don't speak for the Government or post any embarrassing material</li> <li>• Understand the privacy settings and defaults</li> <li>• Consider who you accept as a friend online carefully</li> <li>• Create strong passwords and user names</li> <li>• Beware of links to games, quizzes, advertising, and other applications available through social networking sites</li> <li>• Don't give away your position through GPS or links</li> </ul>
<b>Maintain Situational Awareness</b>	<ul style="list-style-type: none"> <li>• Do not talk about Government business outside Government premises</li> <li>• Remove your security badge when you leave the office</li> <li>• Avoid activities that may compromise situational awareness</li> <li>• Be discreet when retrieving messages from smartphones or other media</li> </ul>
<b>Use Extreme Caution if you Encounter Classified or Other Official Government Documents on the Web</b>	<ul style="list-style-type: none"> <li>• If you encounter classified or other official Government documents not authorized for public release on the Internet: <ul style="list-style-type: none"> <li>○ Do not download it</li> <li>○ Report it to your security POC</li> </ul> </li> </ul>
<b>Be Sensitive to Data Classifications</b>	<ul style="list-style-type: none"> <li>• Avoid sharing sensitive information using shared applications, such as Sharepoint and Google Docs</li> <li>• Be aware that combined non-sensitive information could result in sensitive information</li> </ul>