

301 FW Network Users Quick Reference Card

NETWORK USER “DOs and DON’Ts” All network users help ensure network integrity by following the below “DOs and DON’Ts.” These are all common sense items that, if adhered to, will assist in maintaining network security and help thwart threat attempts by an unknown attacker.

01 Be aware of your surroundings and report suspicious behavior such as “shoulder surfing” or unauthorized access to sensitive or classified information. Challenge unknown personnel in your areas, especially when their behavior is questionable!

02 Never leave your computer unattended without using a password/pin-protected screen saver, removing your common access card (CAC), or logging off the network completely. Never leave your CAC unattended in your computer.

03 Protect your access to information from the insider threat: **DO NOT** share your password/pin. **DO NOT** write your password/pin down so it can be accessed easily. Remember, the first places an intruder will check for your password/pin are the most common places people write them down: (1) on the back of the keyboards, (2) bottom of the mouse, (3) posted on the wall, and (4) printed on a piece of paper laying in a desk drawer.

04 Social engineering is a very large network threat. Social engineering can be accomplished by email, telephone, or even in person. A very common attack is an email asking you to test your password/pin for composition compliance by inserting it in the space provided and pressing enter. There is no reason whatsoever for a network user to provide his or her password/pin. No matter how official the email looks, no matter who the individual says he or she is, and no matter who the individual is in your office—**NEVER** give your password/pin to anyone for any reason. If you are aware of any type of social engineering, immediately contact the communications focal point (CFP), or cyber security office (IAO).

05 Don’t download personal software, games, or programs from the internet without obtaining formal software approval. Why? Some downloaded files may contain malicious logic such as viruses or Trojan Horse programs. Report suspicious computer behavior to the CFP or your IAO.

06 A common threat to our network is a **distributed denial of service (DDoS)** attack. The most common DDoS attacks relate to email. Beware of email from unknown sources or from known individuals but with unusual subjects forwarding an attachment. Many DDoS attacks are triggered by an embedded script in the attachment that goes to your address book and resends the same email, with attachment, to everyone in your address book. If you receive such an email, immediately delete it and notify the CFP or your IAO.

07 Other possible DDoS attacks relate to **Internet hoaxes**. These are warnings of new viruses, moneymaking schemes, or chain letters. They all ask the users to forward the message to friends in the name of a fictitious cause. These types of attacks only slow down the Internet and email service for computer users. Do not respond to these requests. Notify the CFP or your IAO.

08 Ensure you scan all removable media for viruses before accessing. Common symptoms of viruses include: (1) slow performance, (2) files disappearing, (3) constant computer error messages, (4) erratic flashing, or (5) constant email error messages. Contact the CFP or your IAO if you experience any of these problems.

09 What do you do if you are sitting at your computer and suddenly the mouse cursor moves around the screen, and files and programs are being accessed without you doing anything? This could be a security incident—report it to the CFP or your IAO immediately.

Points of Contact:

Communications Focal Point (CFP): **782-7181**

Wing Cyber Security Office (formerly WIAO): **782-5657**

WISSM Secure Terminal Equipment (STE) Number: **782-3041**

301FWVA 33-101 26 May 2016

Supersedes: 301FWVA33-101, 12 May 2014

Prescribed by: AFI33-115

OPR: 301CS/SCXS

301FW Network Users Quick Reference Guide

RELEASABILITY: There are no releasability restrictions on this publication

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing web site at www.e-Publishing.af.mil

301 FW Network Users Quick Reference Card

VIRUS Reporting Procedures: If suspicious or unusual activities occur or there's a suspected virus, DO NOT answer any prompts or messages and complete the following:

Item # Task:

- 01** Stop using the system.
- 02** DO NOT shut off the machine.
- 03** Isolate machine from network by unplugging the network cable at the back of the computer.
- 04** Notify the CFP or your IAO immediately.
- 05** DO NOT attempt to run your AntiVirus client.

Classified Message Incident (CMI): If classified information is accidentally placed on your system or on the local area network, the incident is CLASSIFIED. DO the following immediately:

Item # Task:

- 01** If received via email, document the sender, subject line, time received, any other recipients, and attachment name if it exists. DO NOT disclose the subject line over unsecured media.
- 02** If the document was printed, disconnect the printer and secure it with the computer.
- 03** If found on file servers or on the Web, document where you found it (for example, file path or Web page).
- 04** Notify the CFP or your IAO in person immediately or via secure media (for example, STE). If the CMI occurred on the local machine, physically guard the machine.
- 05** Do not delete the message or file.
- 06** Isolate machine from network by unplugging the network cable at the back of the computer.

DoD Information Assurance Awareness training is required annually:

Notes:

