



LUKE AFB

NETWORK INCIDENT REPORTING AID
OPSEC – DO NOT DISCUSS/TRANSMIT
SENSITIVE INFORMATION OVER
UNAUTHORIZED SYSTEMS



COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

STEP 1	STOP!!! DISCONNECT THE LAN CABLE. Discontinue Use
STEP 2	LEAVE THE SYSTEM POWERED UP. Personnel should <u>not</u> click on any prompts, close any windows, or shut down the system.
STEP 3	If a message appears on the monitor of the affected system - WRITE IT DOWN!
STEP 4	WRITE DOWN ALL ACTIONS that occurred during the suspected virus attack. (Did the virus come from an e-mail attachment, diskette, etc.?)
STEP 5	REPORT IT IMMEDIATELY! Contact your section's Cybersecurity Liaison (CSL).

NOTE: When reporting a suspected virus to your CSL to ensure that you give the following information to the technician:

- Report Date and Time
- Your name, telephone number, bldg, and organization
- Event Date and Time
- Location of infected system(s)

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS

A **CMI** is the introduction of information of a higher classification into a lower classification level computer device.

STEP 1	STOP!!! DISCONNECT THE LAN CABLE of the affected computer system(s) and/or printer(s)
STEP 2	SECURE affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance.
STEP 3	REPORT INCIDENT IMMEDIATELY by telephone or in person to your Security Manager, CSL, and Supervisor. If unavailable, contact the Wing Cybersecurity Office at 6-3560. You may only say, "I'd like to report a possible CMI" via non-secure means and wait for WCSO personnel to

PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH

IAW AFI 33-332, a PII breach is defined as "actual or possible loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic."

STEP 1	STOP!!! Take actions to mitigate further loss or compromise
STEP 2	REPORT INCIDENT IMMEDIATELY by phone/email to the Base Privacy Manager (56 CS/SCOKR) at 6-6571; Unit Privacy Act Monitor (FARM) and your unit Security Manager.
STEP 3	COMPLETE INITIAL PII BREACH REPORT (No names/use positions), Template with instructions located at the AF Privacy Act website, http:// www.privacy.af.mil/helpfulresources/index.asp
STEP 4	SUBMIT INITIAL PII BREACH REPORT WITHIN 12 HOURS to the Base Privacy Manager at heidi.janey.2@us.af.mil.
STEP 5	Base Privacy Manager will validate report and submit to AETC and senior leadership within 24 hours of breach discovery.



LUKE AFB

NETWORK INCIDENT REPORTING AID
OPSEC – DO NOT DISCUSS/TRANSMIT
SENSITIVE INFORMATION OVER
UNAUTHORIZED SYSTEMS



COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

STEP 1	STOP!!! DISCONNECT THE LAN CABLE. Discontinue Use
STEP 2	LEAVE THE SYSTEM POWERED UP. Personnel should <u>not</u> click on any prompts, close any windows, or shut down the system.
STEP 3	If a message appears on the monitor of the affected system - WRITE IT DOWN!
STEP 4	WRITE DOWN ALL ACTIONS that occurred during the suspected virus attack. (Did the virus come from an e-mail attachment, diskette, etc.?)
STEP 5	REPORT IT IMMEDIATELY! Contact your section's Cybersecurity Liaison (CSL).

NOTE: When reporting a suspected virus to your CSL to ensure that you give the following information to the technician:

- Report Date and Time
- Your name, telephone number, bldg, and organization
- Event Date and Time
- Location of infected system(s)

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS

A **CMI** is the introduction of information of a higher classification into a lower classification level computer device.

STEP 1	STOP!!! DISCONNECT THE LAN CABLE of the affected computer system(s) and/or printer(s)
STEP 2	SECURE affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance.
STEP 3	REPORT INCIDENT IMMEDIATELY by telephone or in person to your Security Manager, CSL, and Supervisor. If unavailable, contact the Wing Cybersecurity Office at 6-3560. You may only say, "I'd like to report a possible CMI" via non-secure means and wait for WCSO personnel to

PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH

IAW AFI 33-332, a PII breach is defined as "actual or possible loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic."

STEP 1	STOP!!! Take actions to mitigate further loss or compromise
STEP 2	REPORT INCIDENT IMMEDIATELY by phone/email to the Base Privacy Manager (56 CS/SCOKR) at 6-6571; Unit Privacy Act Monitor (FARM) and your unit Security Manager.
STEP 3	COMPLETE INITIAL PII BREACH REPORT (No names/use positions), Template with instructions located at the AF Privacy Act website, http:// www.privacy.af.mil/helpfulresources/index.asp
STEP 4	SUBMIT INITIAL PII BREACH REPORT WITHIN 12 HOURS to the Base Privacy Manager at heidi.janey.2@us.af.mil.
STEP 5	Base Privacy Manager will validate report and submit to AETC and senior leadership within 24 hours of breach discovery.

**LUKE AFB NETWORK USERS
QUICK REFERENCE CARD**

NETWORK USER "DOs & DON'Ts"

- 1 **Be aware of your surroundings** & 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!
- 2 **Don't ever leave your computer unattended** without locking the system (Windows Key + L), removing your CAC card, or logging off the network completely. Never leave your CAC unattended in your computer.
- 3 A very large network threat is **Social Engineering**. Social Engineering can be accomplished by e-mail, telephone, or even in person. A very common attack is an e-mail asking you to test your password for composition compliance by inserting it in the space provided & pressing enter. There is no reason whatsoever for a network user to provide their password. No matter how official the e-mail looks, no matter who the individual says they are, or no matter whom the individual is in your office---NEVER give your password to anyone for any reason. If you are aware of any type of Social Engineering, immediately contact your Functional System Administrator (FSA), Client Support Technician (CST), or Cybersecurity Liaison (CSL).
- 4 **Don't download or install freeware/shareware** or any other software products without DAA approval.
- 5 **No USB devices** are to be connected to Government systems without authorization. Unauthorized use of USB storage devices will be detected by the Host-Based Security System. Violators will be held accountable. Unauthorized devices include phones, cameras, music players, thumb drives, etc., and may not be plugged in - even for charging.
- 6 Other possible DoS attacks relate to **Internet hoaxes**. These are warnings of new viruses, money making 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 e-mail service for computer users. Do not respond to these requests. Notify your CST or CSL.
- 7 Make sure your **antivirus software is current**. Ensure your system is being scanned for viruses every week, at a minimum. **Ensure you scan all removable media for viruses before use.** Common signs of viruses are: (1) Slow performance, (2) Files disappearing, (3) Constant computer error messages, (4) Erratic flashing, or (5) Constant e-mail error messages. If you experience any of these problems, contact your CST.
- 8 What do you do if you are sitting at your computer and suddenly the mouse cursor moves around the screen & files/programs are being accessed w/out you doing anything? This could be a security incident--report it to your CST immediately.

POINTS OF CONTACT

Primary Cybersecurity Liaison (CSL): _____
Alternate Cybersecurity Liaison (CSL): _____
Wing Cybersecurity Office (WCSO): 856-3560
Communications Focal Point: 856-4400

**LUKE AFB NETWORK USERS
QUICK REFERENCE CARD**

NETWORK USER "DOs & DON'Ts"

- 1 **Be aware of your surroundings** & 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!
- 2 **Don't ever leave your computer unattended** without locking the system (Windows Key + L), removing your CAC card, or logging off the network completely. Never leave your CAC unattended in your computer.
- 3 A very large network threat is **Social Engineering**. Social Engineering can be accomplished by e-mail, telephone, or even in person. A very common attack is an e-mail asking you to test your password for composition compliance by inserting it in the space provided & pressing enter. There is no reason whatsoever for a network user to provide their password. No matter how official the e-mail looks, no matter who the individual says they are, or no matter whom the individual is in your office---NEVER give your password to anyone for any reason. If you are aware of any type of Social Engineering, immediately contact your Functional System Administrator (FSA), Client Support Technician (CST), or Cybersecurity Liaison (CSL).
- 4 **Don't download or install freeware/shareware** or any other software products without DAA approval.
- 5 **No USB devices** are to be connected to Government systems without authorization. Unauthorized use of USB storage devices will be detected by the Host-Based Security System. Violators will be held accountable. Unauthorized devices include phones, cameras, music players, thumb drives, etc., and may not be plugged in - even for charging.
- 6 Other possible DoS attacks relate to **Internet hoaxes**. These are warnings of new viruses, money making 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 e-mail service for computer users. Do not respond to these requests. Notify your CST or CSL.
- 7 Make sure your **antivirus software is current**. Ensure your system is being scanned for viruses every week, at a minimum. **Ensure you scan all removable media for viruses before use.** Common signs of viruses are: (1) Slow performance, (2) Files disappearing, (3) Constant computer error messages, (4) Erratic flashing, or (5) Constant e-mail error messages. If you experience any of these problems, contact your CST.
- 8 What do you do if you are sitting at your computer and suddenly the mouse cursor moves around the screen & files/programs are being accessed w/out you doing anything? This could be a security incident--report it to your CST immediately.

POINTS OF CONTACT

Primary Cybersecurity Liaison (CSL): _____
Alternate Cybersecurity Liaison (CSL): _____
Wing Cybersecurity Office (WCSO): 856-3560
Communications Focal Point: 856-4400