

<b>8<sup>th</sup> Fighter Wing</b> <b>NETWORK INCIDENT REPORTING AID</b> <i>OPSEC-DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS</i>	
INFOCON LEVELS	
Purpose of INFOCON is to provide a framework to increase the measurable readiness of networks to match operational priorities by prescribing actions and cycles necessary for reestablishing the confidence level and security of information systems for the CC.	
<b>INFOCON 5: Routine Setups:</b> Normal readiness of information systems and networks that can be sustained indefinitely. <b>INFOCON 4: Increased Vigilance:</b> In preparation for operations or exercises, with a limited impact to the end user. <b>INFOCON 3: Enhanced Readiness:</b> Increases the frequency of validation of information networks and its corresponding configuration. Impact to end-user is minor. <b>INFOCON 2: Greater Readiness:</b> Increases the frequency of validation of information networks and its corresponding configuration. Impact to administrators will increase and impact to end-user could be significant. <b>INFOCON 1: Maximum Readiness:</b> Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact on administrators and end-users.	
COMPUTER VIRUS REPORTING PROCEDURES FOR USERS	
<b>STEP 1</b>	<b>STOP! DISCONNECT THE LAN CABLE.</b> Discontinue Use
<b>STEP 2</b>	<b>LEAVE THE SYSTEM POWERED UP.</b> Personnel should <u>not</u> click on any prompts, close any windows, or shut down the system.
<b>STEP 3</b>	If a message appears on the monitor of the affected system - <b>WRITE IT DOWN!</b>
<b>STEP 4</b>	<b>WRITE DOWN ALL ACTIONS</b> that occurred during the suspected virus attack. (Did the virus come from an e-mail attachment, diskette, etc..?)
<b>STEP 5</b>	<b>REPORT IT IMMEDIATELY!</b> Contact your section's IAO or Client Support Administrator (CSA) and CS Helpdesk at 782-2666.
<b>NOTE:</b> When reporting a suspected virus to your IAO and the CS Helpdesk ensure that you give the following information to the technician:	
- Event Date and Time                      - Name of your IAO - Report Date and Time                    - Location of infected system(s) - Your name, telephone number, bldg, and organization	
CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS	
A <i>CMI</i> is defined as a classified message that has been sent and/or received over an unclassified network.	
<b>STEP 1</b>	<b>STOP! DISCONNECT THE LAN CABLE</b> of the affected computer system(s) and/or printer(s)
<b>STEP 2</b>	<b>SECURE</b> affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance.
<b>STEP 3</b>	<b>REPORT INCIDENT IMMEDIATELY</b> by telephone or in person to your Security Manager, IAO, CST, Supervisor, and the CS Helpdesk at 782-2666. Note: You may only say, "I'd like to report a possible CMI" via non-secure means and wait for Helpdesk personnel to assist.
<b>8 CS Comm Focal Point: 782-2666</b>	

8FWVA33-1, 6 May 2014, (Prescribed by AF133-101)  
 ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-publishing website at [www.e-Publishing.af.mil](http://www.e-Publishing.af.mil).  
 RELEASABILITY: There are no releasability restrictions on this publication.

**INFOCON PROTECTIVE MEASURES**

---

Use the **proper password** creation methods and utilize **screensaver** passwords under all INFOCON levels. Backup **your data** under all INFOCON levels. Consider more frequent backups as the level heightens. Ensure you have backups of **mission critical data**.  
 During INFOCON 4, passwords must be changed every 90 days instead of every 120. When INFOCON 4 occurs many passwords will **expire** and individuals will be required to change passwords.  
**Report suspicious activity.** As the INFOCON level escalates, personnel should become increasingly mindful of situations that indicate information may be at risk. Stay alert for possible **computer viruses/malicious code attacks and unauthorized persons** asking for potentially sensitive information, i.e. user-ids, passwords, website or E-mail addresses. Heighten your awareness for signs that your E-mail, login account, or other correspondence might have been tampered with or opened.

PHISHING ATTEMPT REPORTING PROCEDURES	
<b>STEP 1</b>	<i>Network Security first!! – DO NOT reply, and never provide CAC PIN to anyone!</i>
<b>STEP 2</b>	<b>Drag email from their Outlook In-Box and SAVE to desktop</b>
<b>STEP 3</b>	<b>Open a new email and address it to helpdesk3@us.af.mil (Create attachment) Attach SAVED email from desktop into new email addressed SPAM/PHISHING Send email. Delete the Spam Email saved on Desktop</b>

NOTES

---

---

---

---

---

---

---

---

---

---

DATE \_\_\_\_\_

OPR: Wing Information Assurance Office, 8 CS/SCXS

**DISPLAY/POST THIS AID NEAR COMPUTER WORKSTATION**