

**341ST MISSILE WING
NETWORK INCIDENT REPORTING AID**

OPSEC – *DO NOT DISCUSS/TRANSMIT CRITICAL INFORMATION VIA NON-SECURE MEANS*

**COMPUTER VIRUS
REPORTING PROCEDURES FOR USERS**

STEP 1	STOP! DISCONNECT THE NETWORK CABLE. <i>Discontinue Use</i>
STEP 2	LEAVE THE SYSTEM POWERED UP. Personnel <i>should not</i> 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. (i.e. Received suspicious e-mail with attachments, Clicked a link, Inserted a disk, Plugged in a USB device; Downloaded a file; etc.)
STEP 5	REPORT IT IMMEDIATELY! Contact your Group Information Assurance Officer (IAO) or the NETSEC Office at 731-2233 .

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

- Event Date and Time
- Your name and telephone number
- Building and room number
- Name of anyone who has assisted you
- Location of infected system

**CLASSIFIED MESSAGE INCIDENT (CMI)
REPORTING PROCEDURES FOR USERS**

A *CMI* is defined as a classified message that has been sent and/or received over an unclassified network.

STEP 1	STOP! DISCONNECT THE LAN CABLE of the affected computer system(s) or printer(s) DO NOT POWER OFF!
STEP 2	REPORT INCIDENT IMMEDIATELY by telephone or in person to WIAO 731-6962, WIP 731-6453, your Security Manager, or Supervisor. Note: You may only say, "I'd like to report a possible CMI" via non-secure means.
STEP 3	SECURE affected system(s) and/or printer(s) in a GSA-approved container or vault, or post a guard with the appropriate clearance, and wait for guidance from WIAO or WIP.

PROTECTIVE MEASURES

Ensure you remove your CAC when leaving your computer unattended.

Backup your data frequently. Consider more frequent backups as the threat levels increase. Ensure you have backups of **mission critical data**.

Report suspicious activity. Personnel should be mindful of situations that indicate information may be at risk. Stay **alert** for possible **computer viruses/malicious code attacks** and **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, share drive, or other correspondence might have been tampered with or opened.

**THE AIR FORCE WILL NEVER ASK FOR YOUR
PASSWORD!!!**

341MWVA33-3 (per AFMAN33-282), 13 July 2012 OPR 341 MW/IA
Supersedes: 341MWVA33-3, 16 July 2009

ACCESSABILITY: This item is accessible from the Malmstrom AFB intranet publications and forms section.

RELEASABILITY: There are no releasability restrictions on this publication.

NOTES

MY INFORMATION ASSURANCE OFFICER (IAO) IS:

MY SECURITY MANAGER IS:



Helpful Phone numbers

Comm Focal Point (CFP):	731-2622
Wing IA:	731-6962/6451
Command Post	731-3801

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