482d FIGHTER WING

NETWORK INCIDENT REPORTING AID

OPSEC – DO NOT DISCUSS/TRANSMIT INFORMATION OVER UNAUTHORIZED SYSTEMS

PHISHING ATTEMPT REPORTING PROCEDURES

Phishing is an attempt to obtain personal or sensitive information through fraudulent emails that try to appear legitimate.

STEP 1: Network Security First!! DO NOT reply & never provide information to unverified email request.

STEP 2: Right click the email, left click junk mail, left click add sender to block sender list, click OK.

STEP 3: Do not forward to others and delete the email, then delete the email in the delete folder.

STEP 4: **REPORT IMMEDIATELY!** Contact the 482 CFP (415-7682).

COMPUTER VIRUS REPORTING PROCEDURES

STEP 1: Stop & Disconnect the LAN cable. Discontinue use of the device.

STEP 2: LEAVE SYSTEM POWER ON.

STEP 3: WRITE DOWN any messages that may appear on the affected system.

STEP 4: REPORT IMMEDIATELY! Contact your Security Manager, Supervisor and 482 CFP (415-7682).

NEGLIGENT DISCHARGE of CLASSIFIED INFORMATION (NDCI) REPORTING PROCEDURES

NDCI: A classified e-mail message that has been sent and /or received over an unclassified network.

STEP 1: Stop & Disconnect the LAN cable. Discontinue use of the device.

STEP 2: SECURE! LOCK WORKSTATION remove your CAC. Stay with the asset until it is placed in an approved GSA container.

STEP 3: Contact your Security Manager, Supervisor and 482 CFP (415-7682).

DATA SPILLAGE REPORTING PROCEDURES

Spillage is a higher classification lever of data place on a lower classification level system or device.

STEP 1: Stop & Disconnect the LAN cable. Discontinue use of the device or system.

STEP 2: SECURE device by staying with the asset until it is place in a GSA container.

STEP 3: Contact your Security Manager, Supervisor and 482 CFP (415-7682)

My Security Manager is:_____

Wing Information Protection (WIPO) 415-6773

482 CS/Communications Focal Point (CFP): 415-7682

Wing Cyber Security Office (WCO): 415-7340

See reverse side for INCIDENT REPORTING CATEGORIES

482 FWVA 33-3 **Prescribed by: AFMAN17-130**

OPR: 482 CS/ SCXS **20200904**

There are no releasability restrictions on this VA

INCIDENT CATEGORIES

CAT I - ROOT LEVEL INTRUSION: Unauthorized entry to root level access privileges on AF computers/information system /network device.

CAT II - USER LEVEL INTRUSION: Unauthorized entry to root level access privileges on AF computers/information system /network device.

CAT III - ATTEMPT ACCESS: Unauthorized persons specifically targets AF computers/information system /network device.

CAT IV - DENIAL OF SERVICE (DOS): Use of AF computers/information system/network device denied due to overwhelming volume of unauthorized traffic.

CAT V - POOR SECURITY PRACTICE: AF information system & network device incorrectly configured or user malice.

CAT VI - SCAN PROBE: Open reports on AF computer/ information system /network device scanned NO DOS or mission impact.

CAT VII - MALICIOUS LOGIC: Hostile code successfully infected AF computers/information system/network device.

INFOCON LEVEL

Presents a structured, coordinated approach to defend against and react to adversarial attacks on DoD computers /telecommunications system and networks. INFOCON levels are as follows:

INFOCON 5: Information networks are operational.

INFOCON 4: Limited risk to ongoing military operations. Operational impact of degradation or loss of information and information systems in low to medium –impact to end-user is NEGLIGIBLE.

INFOCON 3: Risk to mission accomplishment is moderate. Requires vigilance to maintain network security-impact to end-user is MINOR.

INFOCON 2: Risk to mission failure is high. Operational impact of degradation or loss of information is and information system is medium high-impact to end-user could be SIGNIFICANT for short periods which can be migrated training and scheduling.

INFOCON 1: Risk to mission operation is extreme. Operational impact of degradation or loss of information and information systems is high – impact to end-user could be SIGNIFICANT for short periods which can be migrated through training and scheduling.

INFOCON PROTECTIVE MEASURES

Use the proper password creation methods and utilize screensaver passwords under all INFOCON LEVELS. Use CAC logon when possible.

Backup your data under all INFOCON levels. Consider more frequent backups of mission critical data.

During INFOCON 3, passwords must be changed every 45 days instead of every 90 days. When INFOCON 3 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 e-mail addresses. Heighten your awareness for signs that your e-mail, login account, or other correspondence might have been tampered with or opened.

See reverse side for INCIDENT REPORTING ACTIONS

482 FWVA 33-3 **Prescribed by: AFMAN17-130**

OPR: 482 CS/ SCXS **20200904**

There are no releasability restrictions on this VA