All Air Force (AF) Organizations of Joint Base Pearl Harbor-Hickam (JBPHH)

NETWORK INCIDENT REPORTING AID

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

CLASSIFIED MESSAGE INCIDENT (CMI) / SPILLAGE

STEP 1	STOP! Disconnect the LAN cable. DO NOT SHUT DOWN!
STEP 2	SECURE affected system to the classification level of the message. DO NOT LEAVE THE SYSTEM UNSECURE!
STEP 3	DO NOT print the Classified Message, annotating the following: 1. Apparent Classification 2. Email Subject 3. File Name (if applicable) 4. Sender 5. Date/Time of Msg 6. Recipients (including previous email trail) ***Mark your notes with the proper derivative classification***
STEP 4	REPORT IMMEDIATELY by notifying your CL and Security Manager (IN PERSON). Do not discuss the CMI over the phone. If you do not know your CL or Security Manager, call WCO or IP.

COMPUTER VIRUS

STEP 1	STOP! Disconnect the LAN cable
STEP 2	LEAVE THE SYSTEM POWERED UP
STEP 3	WRITE DOWN ALL ACTIONS that occurred as the suspected attack took place. (What sites/programs were in use).
STEP 4	REPORT IMMEDIATELY to Comm Focal Point (447-0737) Inform your CL afterward for proper documentation.

PHISHING/SUSPICIOUS EMAIL

STEP 1	SUBMIT A REPORT using the desktop VESD application

OR

STEP 1	Contact CFP for large-scale phishing attempts

POST THIS AID NEAR COMPUTER SYSTEMS

Cut off/fold this portion and attach to screen-locked monitor for CMIs and Viruses. Remember, if a CMI, a person with adequate clearance must stay with the computer.

NOTES	Use this area to record any known details of incident from STEP 3 (Protect notes that may be classified or sensitive)
1.	
2.	
3.	
4.	
5.	
6.	

All Air Force (AF) Organizations of Joint Base Pearl Harbor-Hickam (JBPHH)

NETWORK INCIDENT REPORTING AID

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

All network users play a role in network integrity by complying with AFI 33-152 User Responsibilities. Below are some items that, if adhered to, will assist in maintaining network security & help thwart threat attempts by an unknown attacker.

1. **Be Aware of your Surroundings** & report suspicious behavior such as "shoulder surfing" or unauthorized access to sensitive or classified information.

2. **Remove your CAC!** Leaving your CAC in a work station creates an end-point security risk.

3. **No Personal Software.** Unapproved software may contain viruses and be harmful to the network.

4. **Only Use Authorized USB or Removable Media Devices!** Never plug in hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar USB storage devices without approval and/or a waiver.

5. **Be Aware of Workstation Settings.** Look for any unusual USB device in your workstation. The Notice and Consent banner should come up on login. The classification banner should appear at the top of your monitor.

6. **Restart Your Computer Daily!** This will ensure: you have the most up-to-date patches, and your computer runs faster.

TEMPEST SEPERATION TIPS

CLASSIFIED DESKTOP/ MONITOR/ PHONE	20 IN or 0.5 METERS	UNCLASSIFIED DESKTOP/ PHONE
CLASSIFIED MONITOR	2 IN or 5cm	UNCLASSIFIED MONITOR
ANY DESKTOP/ MONITOR/ PHONE	2 IN or 5cm	TACLANE/ CRYPTOGRAPHIC EQUIPMENT
CLASSIFIED DESKTOP/ MONITOR/ PHONE	7 FT or 2 METERS	LMR BEFORE TRANSMITTING
CELLPHONES/ PERSONAL ELECTRONIC DEVICES	JUST DON'T DO IT	

JBPEARLHARBOR-HICKAMVA33-138, 9 June 2016 (Per AFI33-138)

OPR: 747 CS/SCXS

ACCESSIBILITY: Publication and forms are available on the e-publishing website at www.e-publishing.af.mil for downloading or ordering RELEASABILITY: There are no releasability restrictions on this publication.

POST THIS AID NEAR COMPUTER SYSTEMS

Cut off/fold this portion and attach to screen-locked monitor for CMIs and Viruses. Remember, if a CMI, a person with adequate clearance must stay with the computer.

INFECTED COMPUTER PLACARD (ICP)

DO NOT USE!!!

CONTACT CL OR CFP PRIOR TO ACCESS

DO NOT POWER DOWN!!!

CONTACT INFORMATION

SECURITY MANAGER	
CL	PRIMARY-
	ALTERNATE-
CSA	PRIMARY-
	ALTERNATE-
CFP	448-0737
WCSO	448-4956

KEEP ASKING UNTIL YOU FIND OUT!

All Air Force (AF) Organizations of Joint Base Pearl Harbor-Hickam (JBPHH)

NETWORK INCIDENT REPORTING AID

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

CLASSIFIED MESSAGE INCIDENT (CMI) / SPILLAGE

STEP 1	STOP! Disconnect the LAN cable. DO NOT SHUT DOWN!
STEP 2	SECURE affected system to the classification level of the message. DO NOT LEAVE THE SYSTEM UNSECURE!
STEP 3	DO NOT print the Classified Message, annotating the following: 1. Apparent Classification 2. Email Subject 3. File Name (if applicable) 4. Sender 5. Date/Time of Msg 6. Recipients (including previous email trail) ***Mark your notes with the proper derivative classification***
STEP 4	REPORT IMMEDIATELY by notifying your CL and Security Manager (IN PERSON). Do not discuss the CMI over the phone. If you do not know your CL or Security Manager, call WCO or IP.

COMPUTER VIRUS

STEP 1	STOP! Disconnect the LAN cable
STEP 2	LEAVE THE SYSTEM POWERED UP
STEP 3	WRITE DOWN ALL ACTIONS that occurred as the suspected attack took place. (What sites/programs were in use).
STEP 4	REPORT IMMEDIATELY to Comm Focal Point (447-0737) Inform your CL afterward for proper documentation.

PHISHING/SUSPICIOUS EMAIL

STEP 1	SUBMIT A REPORT using the desktop VESD application

OR

STEP 1	Contact CFP for large-scale phishing attempts

POST THIS AID NEAR COMPUTER SYSTEMS

Cut off/fold this portion and attach to screen-locked monitor for CMIs and Viruses. Remember, if a CMI, a person with adequate clearance must stay with the computer.

NOTES	Use this area to record any known details of incident from STEP 3 (Protect notes that may be classified or sensitive)
1.	
2.	
3.	
4.	
5.	
6.	

All Air Force (AF) Organizations of Joint Base Pearl Harbor-Hickam (JBPHH)

NETWORK INCIDENT REPORTING AID

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

All network users play a role in network integrity by complying with AFI 33-152 User Responsibilities. Below are some items that, if adhered to, will assist in maintaining network security & help thwart threat attempts by an unknown attacker.

1. **Be Aware of your Surroundings** & report suspicious behavior such as "shoulder surfing" or unauthorized access to sensitive or classified information.

2. **Remove your CAC!** Leaving your CAC in a work station creates an end-point security risk.

3. **No Personal Software.** Unapproved software may contain viruses and be harmful to the network.

4. **Only Use Authorized USB or Removable Media Devices!** Never plug in hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar USB storage devices without approval and/or a waiver.

5. **Be Aware of Workstation Settings.** Look for any unusual USB device in your workstation. The Notice and Consent banner should come up on login. The classification banner should appear at the top of your monitor.

6. **Restart Your Computer Daily!** This will ensure: you have the most up-to-date patches, and your computer runs faster.

TEMPEST SEPERATION TIPS

CLASSIFIED DESKTOP/ MONITOR/ PHONE	20 IN or 0.5 METERS	UNCLASSIFIED DESKTOP/ PHONE
CLASSIFIED MONITOR	2 IN or 5cm	UNCLASSIFIED MONITOR
ANY DESKTOP/ MONITOR/ PHONE	2 IN or 5cm	TACLANE/ CRYPTOGRAPHIC EQUIPMENT
CLASSIFIED DESKTOP/ MONITOR/ PHONE	7 FT or 2 METERS	LMR BEFORE TRANSMITTING
CELLPHONES/ PERSONAL ELECTRONIC DEVICES	JUST DON'T DO IT	

JBPEARLHARBOR-HICKAMVA33-138, 9 June 2016 (Per AFI33-138)

OPR: 747 CS/SCXS

ACCESSIBILITY: Publication and forms are available on the e-publishing website at www.e-publishing.af.mil for downloading or ordering RELEASABILITY: There are no releasability restrictions on this publication.

POST THIS AID NEAR COMPUTER SYSTEMS

Cut off/fold this portion and attach to screen-locked monitor for CMIs and Viruses. Remember, if a CMI, a person with adequate clearance must stay with the computer.

INFECTED COMPUTER PLACARD (ICP)

DO NOT USE!!!

CONTACT CL OR CFP PRIOR TO ACCESS

DO NOT POWER DOWN!!!

CONTACT INFORMATION

SECURITY MANAGER	
CL	PRIMARY-
	ALTERNATE-
CSA	PRIMARY-
	ALTERNATE-
CFP	448-0737
WCSO	448-4956

KEEP ASKING UNTIL YOU FIND OUT!