DAVIS-MONTHAN

NETWORK INCIDENT REPORTING AID

OPSEC – DO NOT DISCUSS/TRANSMIT SENSITIVE INFORMATION OVER UNAUTHORIZED SYSTEMS

CLASSIFIED MESSAGE INCIDENT (CMI) *REPORTING PROCEDURES*

CMI: a classified message sent/received over an unclassified network

STEP 1	STOP! Disconnect the LAN cable
STEP 2	SECURE affected system to the classification level of the message. DO NOT LEAVE THE SYSTEM UNSECURE!
STEP 3	TAKE NOTES 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 CSL and Security Manager (IN PERSON). Do not discuss the CMI over the phone.

COMPUTER VIRUS *REPORTING PROCEDURES*

STEP 1	STOP! DISCONNECT THE LAN CABLE. Discontinue use and isolate system from the network.
STEP 2	LEAVE THE SYSTEM POWERED UP DO NOT click prompts, close windows or shut down the system.
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 (228-7253) Inform your CSL afterward for proper documentation.

PHISHING EMAILS *PROCEDURES*

Phishing: a form of online identity theft where attackers deceive internet users into submitting personal information to illegitimate web sites or through email.

STEP 1	DO NOT RELEASE PERSONAL INFORMATION through the internet/email unless you verify who is receiving the information and the site/email is secure. (i.e. encrypted email, HTTPS site) (NOTE: For general Spam, block the sender and delete message.)
STEP 2	DRAG EMAIL FROM YOUR INBOX TO YOUR DESKTOP to save the email. DO NOT click reply or forward on original email.
STEP 3	ATTACH SAVED EMAIL TO NEW EMAIL and send it to Report.Spam@us.af.mil. Email will be an attachment.

*Emails that contain illegal content, **STOP!** Notify your USM and supervisor.*

INFOCON LEVELS *INFORMATIONAL*

The DoD INFOCON system: a series of prescribed and standardized actions to maintain or re-establish the confidence level of networks under a commander's authority. The INFOCON system incorporates a "readiness-based" strategy.

INFOCON 5	ROUTINE NETWORK OPERATIONS: Normal readiness of Information Systems and networks that can be sustained indefinitely
INFOCON 4	INCREASED VIGILANCE: In preparation for operations or exercises, with a limited impact to the end user.
INFOCON 3	ENHANCED READINESS: Increases the validation frequency of information networks and its corresponding configuration. **Impact to end-user is minor.**
INFOCON 2	GREATER READINESS: Increases validation frequency of information networks and corresponding configuration. Increased impact to administration and **impact to end-user could be significant.**
INFOCON 1	MAXIMUM READINESS: 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.**

DAVISMONTHANAFBVA33-200, 19 July 2016

Prescribed by: TO 00-33B-5007
OPR: 355 CS/SCXS CYBERSECURITY

POST NEAR ALL COMPUTER WORKSTATIONS
Supersedes all previous versions

DAVIS-MONTHAN

NETWORK INCIDENT REPORTING AID

OPSEC – DO NOT DISCUSS/TRANSMIT SENSITIVE INFORMATION OVER UNAUTHORIZED SYSTEMS

CLASSIFIED MESSAGE INCIDENT (CMI) *REPORTING PROCEDURES*

CMI: a classified message sent/received over an unclassified network

STEP 1	STOP! Disconnect the LAN cable
STEP 2	SECURE affected system to the classification level of the message. DO NOT LEAVE THE SYSTEM UNSECURE!
STEP 3	TAKE NOTES 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 CSL and Security Manager (IN PERSON). Do not discuss the CMI over the phone.

COMPUTER VIRUS *REPORTING PROCEDURES*

STEP 1	STOP! DISCONNECT THE LAN CABLE. Discontinue use and isolate system from the network.
STEP 2	LEAVE THE SYSTEM POWERED UP DO NOT click prompts, close windows or shut down the system.
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 (228-7253) Inform your CSL afterward for proper documentation.

PHISHING EMAILS *PROCEDURES*

Phishing: a form of online identity theft where attackers deceive internet users into submitting personal information to illegitimate web sites or through email.

STEP 1	DO NOT RELEASE PERSONAL INFORMATION through the internet/email unless you verify who is receiving the information and the site/email is secure. (i.e. encrypted email, HTTPS site) (NOTE: For general Spam, block the sender and delete message.)
STEP 2	DRAG EMAIL FROM YOUR INBOX TO YOUR DESKTOP to save the email. DO NOT click reply or forward on original email.
STEP 3	ATTACH SAVED EMAIL TO NEW EMAIL and send it to Report.Spam@us.af.mil. Email will be an attachment.

*Emails that contain illegal content, **STOP!** Notify your USM and supervisor.*

INFOCON LEVELS *INFORMATIONAL*

The DoD INFOCON system: a series of prescribed and standardized actions to maintain or re-establish the confidence level of networks under a commander's authority. The INFOCON system incorporates a "readiness-based" strategy.

INFOCON 5	ROUTINE NETWORK OPERATIONS: Normal readiness of Information Systems and networks that can be sustained indefinitely
INFOCON 4	INCREASED VIGILANCE: In preparation for operations or exercises, with a limited impact to the end user.
INFOCON 3	ENHANCED READINESS: Increases the validation frequency of information networks and its corresponding configuration. **Impact to end-user is minor.**
INFOCON 2	GREATER READINESS: Increases validation frequency of information networks and corresponding configuration. Increased impact to administration and **impact to end-user could be significant.**
INFOCON 1	MAXIMUM READINESS: 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.**

DAVISMONTHANAFBVA33-200, 19 July 2016

Prescribed by: TO 00-33B-5007
OPR: 355 CS/SCXS CYBERSECURITY

POST NEAR ALL COMPUTER WORKSTATIONS
Supersedes all previous versions

DAVIS-MONTHAN

NETWORK INCIDENT REPORTING AID

NETWORK USER "DOs & DON'Ts"

INTRODUCTION: All network users play a role in network integrity by complying with AFI 33-152 User Responsibilities. Below are some common-sense 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. Challenge unknown personnel in your areas, especially when their behavior is questionable!

2. **Remove your CAC!** Never leave your CAC unattended in your computer. If your workstation does not lock when CAC is removed, report it to your CSL.

3. **No Personal Software.** Don't download personal software, games or programs from the Internet without obtaining formal software approval.

4. **No Unauthorized USB or Removable Media Devices!** Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar USB storage devices.

5. **Delete generic Spam and Chain Letters.** Chain letters in HTML or with hyperlinks can contain malware and is not worth the risk.

6. **Be Aware of Workstation Settings.** There should not be 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. If there are any abnormalities, report them to your CSL.

7. **Restart Your Computer Daily!** This will ensure: you have the most up-to-date patches, your computer runs faster, and you don't lose data with the 72-hour force restart implementation.

8. **For more information** on Davis-Monthan User information, refer to the Cybersecurity SharePoint at https://dm.eim.acc.af.mil/355MSG/355CS/SCX/SCXS/default.aspx

IMPORTANT POINTS OF CONTACT

Cybersecurity Office (WCO):	228-5314 355CS/SCXS@us.af.mil
Communications Focal Point (CFP):	228-7253
Wing Information Protection (IP):	228-3708

UNIT INFORMATION *(Optional)*

Cybersecurity Liaisons (CSL)

Primary : ______________________
Alternate: ______________________
Alternate: ______________________
Alternate: ______________________

MDG
DO NOT USE
FOLLOW PROPRIETARY PROCEDURES

The vESD app can be used to report incidents and help with any other network issues!

DAVISMONTHANAFBVA33-200, 19 July 2016
Prescribed by: TO 00-33B-5007

OPR: 355 CS/SCXS CYBERSECURITY
POST NEAR ALL COMPUTER WORKSTATIONS
Supersedes all previous versions

DAVIS-MONTHAN
NETWORK INCIDENT REPORTING AID
NETWORK USER "DOs & DON'Ts"

INTRODUCTION: All network users play a role in network integrity by complying with AFI 33-152 User Responsibilities. Below are some common-sense 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. Challenge unknown personnel in your areas, especially when their behavior is questionable!

2. **Remove your CAC!** Never leave your CAC unattended in your computer. If your workstation does not lock when CAC is removed, report it to your CSL.

3. **No Personal Software.** Don't download personal software, games or programs from the Internet without obtaining formal software approval.

4. **No Unauthorized USB or Removable Media Devices!** Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar USB storage devices.

5. **Delete generic Spam and Chain Letters.** Chain letters in HTML or with hyperlinks can contain malware and is not worth the risk.

6. **Be Aware of Workstation Settings.** There should not be 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. If there are any abnormalities, report them to your CSL.

7. **Restart Your Computer Daily!** This will ensure: you have the most up-to-date patches, your computer runs faster, and you don't lose data with the 72-hour force restart implementation.

8. **For more information** on Davis-Monthan User information, refer to the Cybersecurity SharePoint at https://dm.eim.acc.af.mil/355MSG/355CS/SCX/SCXS/default.aspx

IMPORTANT POINTS OF CONTACT

Cybersecurity Office (WCO): 228-5314 355CS/SCXS@us.af.mil
Communications Focal Point (CFP): 228-7253
Wing Information Protection (IP): 228-3708

UNIT INFORMATION *(Optional)*

Cybersecurity Liaisons (CSL)

Primary : ______________________
Alternate: ______________________
Alternate: ______________________
Alternate: ______________________

MDG
DO NOT USE
FOLLOW PROPRIETARY PROCEDURES

The vESD app can be used to report incidents and help with any other network issues!

DAVISMONTHANAFBVA33-200, 19 July 2016
Prescribed by: TO 00-33B-5007

OPR: 355 CS/SCXS CYBERSECURITY
POST NEAR ALL COMPUTER WORKSTATIONS
Supersedes all previous versions