SHEPPARD AFB
NETWORK INCIDENT REPORTING AID

OPSEC – Do not discuss/transmit sensitive information over unauthorized systems

NEGLIGENT DISCHARGE OF CLASSIFIED INFORMATION (NDCI) (Previously CMI) *REPORTING PROCEDURES*

NDCI: Classified content released to an unclassified system/network/message

STEP 1	**STOP!** Do not delete message(s). DISCONNECT THE LAN CABLE OF AFFECTED SYSTEM(S)!
STEP 2	**SECURE** affected system(s) in a GSA-approved safe/vault, certified secure room, or with a person possessing an appropriate clearance. DON'T 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 as "Classified Working Paper" and secure IAW STEP 2*
STEP 4	**REPORT IMMEDIATELY** by notifying your Unit SA and the CFP (IN PERSON) and provide notes. DON'T DISCUSS THE INCIDENT OVER THE PHONE!

COMPUTER VIRUS *REPORTING PROCEDURES*

STEP 1	**STOP! DO NOT CHANGE ANYTHING** Windows Security and AFNet Security may be working in the background.
STEP 2	**WRITE DOWN ALL ACTIONS** and information, including error codes, that occurred. (What sites/programs were in use).
STEP 3	**REPORT IMMEDIATELY** to Comm Focal Point (676-HELP) Inform your CL afterward for situational awareness.

PHISHING/SPAM 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	**OPEN A NEW EMAIL** and drag/drop the suspected email as an attachment. DO NOT click reply or forward on original email.
STEP 3	**SEND** new email to **Sheppard.Spam@us.af.mil**. Email will be an attachment.

*Emails that contain illegal content: **STOP!** Notify your SA and supervisor.*

CPCON LEVELS *INFORMATIONAL*

USCYBERCOM Instruction 5200-13 establishes Cyberspace Protection Conditions (CPCON) for the DoD. CPCON establishes protection priorities for each level during significant cyberspace events, as shown in the table below. Depending on the CPCON level, users may experience disruptions in service or access to physical spaces.

CPCON 5	**Very Low:** Critical Functions
CPCON 4	**Low:** Critical and Essential Functions.
CPCON 3	**Medium:** Critical, Essential, and Support Functions
CPCON 2	**High:** Critical and Essential Functions
CPCON 1	**Very High:** Critical Function

SHEPPARDAFBVA17-130, 20230525
OPR: 82 CS/SCXS CYBERSECURITY
Supercedes SAFB VA 17-130, 20190709
Prescribing Directive: AFI17-130
RELEASABILITY: There are not releasability restrictions on the publication.

SHEPPARD AFB
NETWORK INCIDENT REPORTING AID
OPSEC – Do not discuss/transmit sensitive information over unauthorized systems
NEGLIGENT DISCHARGE OF CLASSIFIED INFORMATION (NDCI) (Previously CMI) REPORTING PROCEDURES
NDCI: Classified content released to an unclassified system/network/message
STEP 1 STOP! Do not delete message(s). DISCONNECT THE LAN CABLE OF AFFECTED SYSTEM(S)!
STEP 2 SECURE affected system(s) in a GSA-approved safe/vault, certified secure room, or with a person possessing an appropriate clearance. DON'T 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 as "Classified Working Paper" and secure IAW STEP 2
STEP 4 REPORT IMMEDIATELY by notifying your Unit SA and the CFP (IN PERSON) and provide notes. DON'T DISCUSS THE INCIDENT OVER THE PHONE!
COMPUTER VIRUS REPORTING PROCEDURES
STEP 1 STOP! DO NOT CHANGE ANYTHING
Windows Security and AFNet Security may be working in the background.
STEP 2 WRITE DOWN ALL ACTIONS and information, including error codes, that occurred. (What sites/programs were in use).
STEP 3 REPORT IMMEDIATELY to Comm Focal Point (676-HELP) Inform your CL afterward for situational awareness.
PHISHING/SPAM 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 OPEN A NEW EMAIL and drag/drop the suspected email as an attachment. DO NOT click reply or forward on original email.
STEP 3 SEND new email to Sheppard.Spam@us.af.mil. Email will be an attachment.
Emails that contain illegal content: STOP! Notify your SA and supervisor.
CPCON LEVELS INFORMATIONAL
USCYBERCOM Instruction 5200-13 establishes Cyberspace Protection Conditions (CPCON) for the DoD. CPCON establishes protection priorities for each level during significant cyberspace events, as shown in the table below. Depending on the CPCON level, users may experience disruptions in service or access to physical spaces.
CPCON 5 Very Low: Critical Functions
CPCON 4 Low: Critical and Essential Functions.
CPCON 3 Medium: Critical, Essential, and Support Functions
CPCON 2 High: Critical and Essential Functions
CPCON 1 Very High: Critical Function
SHEPPARDAFBVA17-130, 20230525
OPR: 82 CS/SCXS CYBERSECURITY
Supercedes SAFB VA 17-130, 20190709
Prescribing Directive: AFI17-130
RELEASABILITY: There are not releasability restrictions on the publication.

SHEPPARD AFB

NETWORK INCIDENT REPORTING AID

NETWORK USER "DOs & DON'Ts"

INTRODUCTION: All network users play a role in network integrity by complying with security policy. 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 or outside your positive control. If your workstation does not lock when CAC is removed, report it to your CL. Also, never share your PIN with anyone.

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 ISSO.

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 Sheppard AFB User information, refer to the Cybersecurity SharePoint site (https://cs2.eis.af.mil/sites/11448/default.aspx).

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

IMPORTANT POINTS OF CONTACT

Wing Cybersecurity Office (WCO): 676-6828 82TRW.IA@us.af.mil

Communications Focal Point (CFP): 676-HELP (4357)

Wing Information Protection (IP): 676-3514 82TRW.IP@us.af.mil

UNIT INFORMATION *(Optional)*

Unit: _____ **CYBERSECURITY LIAISON (CL)**

Primary CL: _____

Alternate CL: _____

Unit Security Manager: _____

Unit Security Manager: _____

INFECTED COMPUTER PLACARD (ICP)

DO NOT USE!!!

CONTACT ISSO OR CFP PRIOR TO ACCESS

DO NOT POWER DOWN!!!

SHEPPARDAFBVA17-130, 20230525
OPR: 82 CS/SCXS CYBERSECURITY
Supercedes SAFB VA 17-130, 20190709
Prescribing Directive: AFI17-130
RELEASABILITY: There are not releasability restrictions on the publication.

POST NEAR ALL COMPUTER WORKSTATIONS

SHEPPARD AFB

NETWORK INCIDENT REPORTING AID

NETWORK USER "DOs & DON'Ts"

INTRODUCTION: All network users play a role in network integrity by complying with security policy. 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 or outside your positive control. If your workstation does not lock when CAC is removed, report it to your CL. Also, never share your PIN with anyone.

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 ISSO.

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 Sheppard AFB User information, refer to the Cybersecurity SharePoint site (https://cs2.eis.af.mil/sites/11448/default.aspx).

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

IMPORTANT POINTS OF CONTACT

Wing Cybersecurity Office (WCO): 676-6828 82TRW.IA@us.af.mil

Communications Focal Point (CFP): 676-HELP (4357)

Wing Information Protection (IP): 676-3514 82TRW.IP@us.af.mil

UNIT INFORMATION *(Optional)*

Unit: _____ CYBERSECURITY LIAISON (CL)

Primary CL: _____

Alternate CL: _____

Unit Security Manager: _____

Unit Security Manager: _____

INFECTED COMPUTER PLACARD (ICP)

DO NOT USE!!!

CONTACT ISSO OR CFP PRIOR TO ACCESS

DO NOT POWER DOWN!!!

SHEPPARDAFBVA17-130, 20230525
OPR: 82 CS/SCXS CYBERSECURITY
Supercedes SAFB VA 17-130, 20190709
Prescribing Directive: AFI17-130
RELEASABILITY: There are not releasability restrictions on the publication.

POST NEAR ALL COMPUTER WORKSTATIONS