OFFUTT AFB

NETWORK INCIDENT REPORTING AID

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

NEGLIGENT DISCHARGE of CLASSIFIED INFORMATION (NDCI)

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

STEP 1	**STOP! Do not delete or recall the Message/File. DISCONNECT THE LAN CABLE of the affected computer system(s) and/or printer(s).**
STEP 2	**SECURE affected system(s) and/or printer(s) in a GSA-approved container, vault, or post a guard with the appropriate clearance.**
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)** **7) ***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	If a message appears on the monitor of the affected system - ***WRITE IT DOWN!***
STEP 4	***WRITE DOWN ALL ACTIONS*** that occurred as the suspected attack took place. (What sites/programs were in use)
STEP 5	**REPORT IMMEDIATELY** to CYOC (294-2666) Inform your CSL afterward for proper documentation.

NOTE: When reporting a suspected virus, ensure you give the following information to the technician:

- Event date & time
- All information gathered in Steps 3 and 4
- Location of infected system (Bldg, room, cubicle)
- Name of your ISSM
- Your name, phone #, and organization

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.*

USER PII BREACH REPORTING

PII Breach: Loss of control, compromise, unauthorized access/acquisition or disclosure of PII.

STEP 1	**Identify the information as PII**. Verify the information was sent to a non-DoD email address or person who did not have a need to know.
STEP 2	***Do not delete any email traffic.*** Immediately attempt to safeguard the information: recall the message, inform recipients not to forward or allow others to view. Track/annotate whom you have contacted. Also, notify the Wing Privacy Manager 294-1066.

OFFUTT AFB VA 33-7, 12 April 2024
Prescribed by: AFMAN 17-1301, OPR: 55 CYS/CYES
POST NEAR ALL COMPUTER WORKSTATIONS
Supersedes all previous versions

OFFUTT AFB

NETWORK INCIDENT REPORTING AID

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

NEGLIGENT DISCHARGE of CLASSIFIED INFORMATION (NDCI)

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

STEP 1	**STOP! Do not delete or recall the Message/File. DISCONNECT THE LAN CABLE of the affected computer system(s) and/or printer(s).**
STEP 2	**SECURE affected system(s) and/or printer(s) in a GSA-approved container, vault, or post a guard with the appropriate clearance.**
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)** **7) ***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	If a message appears on the monitor of the affected system - ***WRITE IT DOWN!***
STEP 4	***WRITE DOWN ALL ACTIONS*** that occurred as the suspected attack took place. (What sites/programs were in use)
STEP 5	**REPORT IMMEDIATELY** to CYOC (294-2666) Inform your CSL afterward for proper documentation.

NOTE: When reporting a suspected virus, ensure you give the following information to the technician:

- Event date & time
- All information gathered in Steps 3 and 4
- Location of infected system (Bldg, room, cubicle)
- Name of your ISSM
- Your name, phone #, and organization

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.*

USER PII BREACH REPORTING

PII Breach: Loss of control, compromise, unauthorized access/acquisition or disclosure of PII.

STEP 1	**Identify the information as PII**. Verify the information was sent to a non-DoD email address or person who did not have a need to know.
STEP 2	***Do not delete any email traffic.*** Immediately attempt to safeguard the information: recall the message, inform recipients not to forward or allow others to view. Track/annotate whom you have contacted. Also, notify the Wing Privacy Manager 294-1066.

OFFUTT AFB VA 33-7, 12 April 2024
Prescribed by: AFMAN 17-1301, OPR: 55 CYS/CYES
POST NEAR ALL COMPUTER WORKSTATIONS
Supersedes all previous versions

OFFUTT AFB
NETWORK INCIDENT REPORTING AID
NETWORK USER "DOs & DON'Ts"

INTRODUCTION: All network users play a role in network integrity by complying with the AFMAN 17-1301. 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 smart watches, cell phones, 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 force restart implementation.
8. **For more information** on User Information, refer to the Cybersecurity Sharepoint at: https://usaf.dps.mil/teams/IACE/SitePages/Home.aspx

IMPORTANT POINTS OF CONTACT

Cybersecurity Office (WCO): 294-7711 55WG.IA@us.af.mil

Cyber Operations Center (CYOC): 294-2666

Wing Information Protection (IP): 294-5252

UNIT INFORMATION *(Optional)*

Cybersecurity Liaisons (CSL)

Primary:
Alternate:
Alternate:
Alternate:

OFFUTT AFBVA33-7, 12 April 2024
Prescribed by: AFMAN 17-1301, OPR: 55 CYSCYES
POST NEAR ALL COMPUTER WORKSTATIONS
Supersedes all previous versions

OFFUTT AFB
NETWORK INCIDENT REPORTING AID
NETWORK USER "DOs & DON'Ts"

INTRODUCTION: All network users play a role in network integrity by complying with the AFMAN 17-1301. 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 watches, cell phones, 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 force restart implementation.
8. **For more information** on User Information, refer to the Cybersecurity Sharepoint at: https://usaf.dps.mil/teams/IACE/SitePages/Home.aspx

IMPORTANT POINTS OF CONTACT

Cybersecurity Office (WCO): 294-7711 55WG.IA@us.af.mil

Cyber Operations Center (CYOC): 294-2666

Wing Information Protection (IP): 294-5252

UNIT INFORMATION *(Optional)*

Cybersecurity Liaisons (CSL)

Primary:
Alternate:
Alternate:
Alternate:

OFFUTT AFBVA33-7, 12 April 2024
Prescribed by: AFMAN 17-1301, OPR: 55 CYSCYES
POST NEAR ALL COMPUTER WORKSTATIONS
Supersedes all previous versions