RAMSTEIN AIR BASE COMPUTER EMERGENCY QUICK RESPONSE AID

VIRUS/NETWORK ATTACK SYMPTOMS

AFI 17-203 (Cyber Incident Handling), 3.3. Detection and Reporting of Events

- Request To Provide, Reset, Or Change Password
- E-mail From Unfamiliar Source
- Notification Of Logon Attempts By Unknown User
- Unexplained Inability To Log On
- Unexplained New Files
- Unfamiliar File Names
- Inability To Save Files
- Unexplained Modifications or Deletion of Data
- Unfamiliar Error Messages
- Denial Of Service With no CFP NOTAM or notification
- Sudden Lack Of Hard Drive Space or Out of Memory Notification
- Computer Continually Restarts

VIRUS/NETWORK ATTACK RESPONSE

STEP 1	STOP USING THE COMPUTER IMMEDIATELY!!!
STEP 2	**DO NOT** Immediately disconnect or power off until further directed unless the system begins performing destructive tasks: (ie. deleting files or formatting drives).
STEP 3	**DO NOT** Log Off.
STEP 4	**DO NOT** Attempt to run the local anti-virus software.
STEP 5	Contact your Unit Cybersecurity Representative (UCR) or Unit Security Manager (USM) as soon as possible (upon detection). If unavailable, notify the 86 CS Comm Focal Point (via a **SECURE LINE** if possible)
STEP 6	Ensure no one uses the computer.
STEP 7	Follow the instructions of your UCR or USM; write down all of the information regarding the incident and any behaviors observed.
STEP 8	Your UCR may have you complete a statement regarding the incident. Ensure you write down all information you can think of that might be pertinent.

Full listing of UCRs can be found at:

https://usaf.dps.mil/sites/86CS/SCX/SCXS/SitePages/UCR.aspx#ucr-roster

NOTE: When reporting a suspected virus to your UCR, USM, or CFP, ensure you provide the following information:

- Event date and time
- Your name and telephone number
- Building and room number
- Name of anyone who has assisted you
- Location of infected system

POINTS OF CONTACT

1. PRIMARY UNIT CYBERSECURITY POC	PHONE:
2. ALTERNATE UNIT CYBERSECURITY POC	PHONE:
3. PRIMARY SECURITY MANAGER	PHONE:
4. **COMM FOCAL POINT DSN:**	**NIPR: 480-2666** **SIPR: 480-5000**

NEGLIGENT DISCHARGE OF CLASSIFIED INFORMATION (NDCI) RESPONSE

An NDCI occurs when there is classified info on a system that is not approved nor authorized to contain that level of classification

STEP 1	STOP USING THE COMPUTER!
STEP 2	**DO NOT** DISCONNECT NETWORK CABLE.
STEP 3	**DO NOT** Power Off.
STEP 4	**DO NOT** Log Off Immediately.
STEP 5	Do not delete, print, or forward the message.
STEP 6	Do not leave the PC unattended. The person protecting it should be cleared to the level of the message.
STEP 7	Immediately contact your Unit Cybersecurity Representative (UCR) and Security Manager in the order on this card. **DO NOT** mention that you suspect an NDCI has occurred until area is secured or you are on a **SECURE LINE**.

Treat information regarding the NDCI at the same level of classification as the indicent. Isolate all external media used (disks, CDs, etc.)

SUSPICIOUS E-MAIL OR SPAM RESPONSE

If you receive suspicious e-mails (including spam & phishing emails) , do not click on attachments or links. Open the vESD Application. Select More. Select Cyber Threat and proceed to fill out the ticket. Notify UCR, then delete the e-mail once instructed.

CPCON LEVELS

CPCON: is a systematic process for AO Commanders/Directors to adjust protection postures on the DoDIN.

CPCON 5: Risk to mission is very low and applies when there is non-specific threat of adversarial activity with limited consequences.
CPCON 4: Risk to mission is low and applies when there is a specific threat of adversarial activity with limited consequences.
CPCON 3: Risk to mission is high and applies when there is a severe, credible threat of adversarial activity with significant consequences.
CPCON 2: Risk to mission is high and applies when there is a severe, credible threat of adversarial activity with severe consequences.
CPCON 1: Risk to mission is very high and applies when a grave, credible threat of adversarial activity exists with catastrophic consequences.

MARK/REVIEW EMAILS CONTAINING THE FOLLOWING:

- Controlled Unclassified Information (CUI)
- Privacy Act Information
- Personally Identifiable Information (PII)
- Individually identifiable health, DoD payroll, finance, logistics, personnel mgmt, proprietary and foreign gov't info
- Contract data
- Export controlled technical data or information
- Operations Security (OPSEC) information.
- Info specified for encryption (eg. Critical Information List)

PERSONAL INFO: ADDITIONAL GUIDANCE

"A PII breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose." – AFI 33-332 *Para*. 3.1.1. 10 Mar 20

PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH

- **STOP:** Take actions to prevent further loss or compromise, e.g., do not forward the email, share the documents etc.
- **REPORT INCIDENT IMMEDIATELY** by phone to Knowledge Management Office (480-2666 Option 3, Option 3)
- Knowledge Management will review within 24 hours

RAMSTEINABVA17-1, 11 November 2023:
Prescribed Publication AFI17-203)