DISPLAY THIS AID
NEAR COMPUTER WORKSTATION

BEALE AFB NETWORK AID
CYBER EVENT RESPONSE PROCEDURES

SUSPICIOUS E-MAIL AND SPAM RESPONSE

DO NOT CLICK ON ATTACHMENTS OR LINKS

1. Use the vESD desktop icon to open a Cyber Threat ticket
2. In the inbox, right-click the email, select “Junk” > “Block Sender”

COMMON VIRUS/NETWORK ATTACK SYMPTOMS

Requests To Provide, Reset, Or Change Password

- Continually Restarting
- Unexplained New Files
- Inability To Save Files
- Unexplained Changes to Data
- Unfamiliar Error Messages
- Denial Of Service
- Continually Restarting
- Difficulty Printing
- Out-of-Memory Error
- Inability To Log On

VIRUS/NETWORK ATTACK RESPONSE

Step 1	STOP USING THE COMPUTER IMMEDIATELY!!! - DISCONNECT NETWORK CABLE - DO NOT POWER OFF - DO NOT LOG OFF
Step 2	Run an on demand scan on your PC by clicking the file explorer, then clicking on “This PC”, right clicking on Windows (C:) and selecting “Scan for Threats” - When the scan completes verify there are no viruses and plug your PC back in. - If viruses are detected, continue to Step 3.
Step 3	If there were viruses detected, immediately contact the Communications Focal Point listed at the bottom of this card and ensure no one uses the computer.
Step 4	Follow the instructions of the Communications Focal Point Technician; write down all of the information regarding the incident and any behaviors observed.

You may be required to complete a statement regarding the incident. Ensure you write down all information you can think of that might be pertinent.

NEGLIGENT DISCLOSURE OF CLASSIFIED INFORMATION RESPONSE (NDCI)

Formally CMI (Classified Message Incident), an NDCI occurs when a higher classification level of data is on a lower classification system

Step 1	STOP USING THE COMPUTER IMMEDIATELY!!! - DISCONNECT NETWORK CABLE - DO NOT POWER OFF - DO NOT LOG OFF
Step 2	DO NOT delete, print, or forward the message.
Step 3	DO NOT leave the computer unattended. The person protecting it should be cleared to the level of the message.
Step 4	Immediately contact the CFP to inform them that a cyber event occurred which requires immediate attention
Step 5	Follow the instructions of the Communications Focal Point Technician; write down all of the information regarding the incident and any behaviors observed. - DO NOT MENTION that you suspect an NDCI has occurred unless the area is secured and you are on a SECURE LINE.

Treat information regarding the NDCI at the same level of classification as the NDCI and protect all involved media

9 RW CYBER EVENT POINT OF CONTACT
Communications Focal Point
9CS.CFP@us.af.mil DSN 634-2666

OPR:9 RW Wing Cybersecurity Office
BEALEAFBVA33-1, 20231212 Prescribing Directive: AFMAN17-1301
RELEASABILITY: There are no releasability restrictions on this publication.

DISPLAY THIS AID
NEAR COMPUTER WORKSTATION

BEALE AFB NETWORK AID
CYBER SECURITY REMINDERS

AIR FORCE NETWORK RULES OF BEHAVIOR

ALL USERS OF AIR FORCE INFORMATION TECHNOLOGY AGREE TO ACT IN ACCORDANCE WITH THE FOLLOWING AS A CONDITION OF ACCESS:

1. **I WILL** adhere to and actively support all legal, regulatory, and command requirements
2. **I WILL** use the system in a manner that protects information confidentiality, integrity and/or availability
3. **I WILL** protect the physical integrity of computing resources entrusted to my custody or use
4. **I WILL NOT** attempt to exceed my authorized privileges
5. **I WILL NOT** use systems in a way that brings discredit on AF users or the AF, or degrade AF missions
6. **I WILL NOT** waste system and network resources
7. **I WILL NOT connect any device to an AF IT device without coordination and approval from the 9th Comm Squadron.**

CPCON LEVELS

Cyberspace Protection Conditions (CPCON) system presents a structured, coordinated approach to defend against and react to attacks on DoD computer/telecommunication systems and networks.

CPCON Level	Mission Risk	Function Priority	User Impact
CPCON 1	Very High	Critical	Significant
CPCON 2	High	Critical, Essential	Moderate
CPCON 3	Medium	Critical, Essential, Support	Minimal
CPCON 4	Low	All Functions	None
CPCON 5	Very Low	All Functions	None

As the CPCON escalates, personnel should be increasingly mindful of cyber threats that indicate information may be at risk.

Stay alert for unauthorized persons requesting sensitive information (passwords, email addresses, log in precedures etc).

WEBCAM AND VIDEO SECURITY

ALL CAMERAS AND MICROPHONES SHOULD BE COVERED AND / OR DISCONNECTED WHEN NOT IN USE

Prior to each video session, users are required to inspect all space visible from the camera, to include desks, tables, walls, the floor or shred bins, and remove or sufficiently cover all sensitive or classified information to prevent unauthorized disclosure.

CLASSIFIED PROCESSING AREA SECURITY

- Classified Processing Areas are authorized to process classified information, often in conjunction with unclassified information
- **Do not add or relocate any electronics within the space without authorization from the Wing Cybersecurity Office**
- Follow all security countermeasures referenced in the memorandum posted within the space.
- **Unclassified collaborative peripheral devices in mixed classification enviroments are required to be physically disabled unless uniquely reviewed and authorized by WCO**

9 RW CYBERSECURITY POINT OF CONTACT
Wing Cybersecurity Office
9RW.Cybersecurity@us.af.mil DSN 634-3185

OPR:9 RW Wing Cybersecurity Office
BEALEAFBVA33-1, 20231212 Prescribing Directive: AFMAN17-1301
RELEASABILITY: There are no releasability restrictions on this publication.