4th Communications Squadron
NETWORK INCIDENT REPORTING AID
OPSEC – *DO NOT DISCUSS/TRANSMIT SENSITVE INFORMATION OVER UNAUTHORIZED SYSTEMS*

SUSPECTED COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

STEP 1	***STOP!*** **DISCONNECT THE LAN CABLE** *Discontinue use* of the system.
STEP 2	***LEAVE THE SYSTEM POWERED UP.*** **DO NOT** click on any prompts, close any windows, or shut down the system.
STEP 3	***WRITE IT DOWN!*** Record notes on reverse side. The CFP or unit CSL will need the details that occurred during or led to the suspected virus attack. (i.e. Received suspicious e-mail with attachments; Inserted unchecked disk; Downloaded unchecked files; etc.)
STEP 4	***REPORT IT IMMEDIATELY!*** Contact the Comm Focal Point (CFP) immediately and involve your unit CSL as soon as is reasonable (See contact info on Reverse Side)

NOTE: When reporting a suspected virus to your CSL or the CFP ensure that you record notes as needed on reverse side of this form and provide the technician with Your Name and Number.

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS

A *CMI* is defined as a classified message that has been sent and/or received over an unclassified network or network of lower classification.

STEP 1	***STOP!*** **DISCONNECT LAN CABLE** *Discontinue use* of the system and **DO NOT** print the classified message unless directed to do so.
STEP 2	**SECURE** affected system(s) / printer(s), area / room. Limit the exposure of the CMI. **DO NOT** leave the system unsecured. Ensure all affected equipment remains under positive control of authorized personnel.
STEP 3	**TAKE NOTES** annotate the following: Apparent classification, Email Subject, file name, sender, date/time of msg, recipients. ***Mark your notes with the proper derivative classification***
STEP 4	**REPORT INCIDENT IMMEDIATELY** **DO NOT** discuss details of the CMI over unsecure lines. Call the CFP (See contact info on Reverse Side), your unit CSL, Supervisor and your Unit Security Manager

THE PHISHING THREAT IS REAL
STOP, THINK, before you CLICK

- No Airman is Entirely Safe from Phishing w/ targeted Social Engineering
- *Up to 80% of all malware attacks initiated through phishing attempts*
  - *-- Seeking PII, Access to Netwk, Operational Info, Delivery of Malware*
  - *-- Result: ID Theft, financial fraud, espionage, loss of Network/Data*

Three Steps of Phishing
- **The Lure - an enticement to give info/open a link or attachment**
- **The Hook - enticement prompts you to act, click the link/attach**
- **The Catch - info collected/malware planted/access gained**

Recognize Phishing Emails: (May contain these and/or other traits)
- Poses as Position of Authority/Expertise (Government or Commercial)
- Entices you to act now to avoid consequence or to gain reward
- Not from an individual and/or No Digital Signature
- Contains Grammatical Errors or Awkward/Uncommon Wording
- Web address link that shows a diff address when cursor is over link
- Improper/missing signature block or contact info
- Official/urgent email correspondence from gmail or similar service

Report Phishing:
- **DELETE** Suspicious Emails. May try to contact sender using contact info from other source (i.e. GAL) to validate email
- **REPORT** Reoccurring Phishing Emails. Use vESD link on desktop (Cyber Threat button) or Call CFP (See contact info on reverse)

June 2020

Prescribed by AFMAN 17-1301
Distribution: F

SEYMOURJOHNSONAFBVA33-200, 20210603

4th Communications Squadron
NETWORK INCIDENT REPORTING AID
OPSEC – *DO NOT DISCUSS/TRANSMIT SENSITVE INFORMATION OVER UNAUTHORIZED SYSTEMS*

SUSPECTED COMPUTER VIRUS REPORTING PROCEDURES FOR USERS

STEP 1	***STOP!*** **DISCONNECT THE LAN CABLE** *Discontinue use* of the system.
STEP 2	***LEAVE THE SYSTEM POWERED UP.*** **DO NOT** click on any prompts, close any windows, or shut down the system.
STEP 3	***WRITE IT DOWN!*** Record notes on reverse side. The CFP or unit CSL will need the details that occurred during or led to the suspected virus attack. (i.e. Received suspicious e-mail with attachments; Inserted unchecked disk; Downloaded unchecked files; etc.)
STEP 4	***REPORT IT IMMEDIATELY!*** Contact the Comm Focal Point (CFP) immediately and involve your unit CSL as soon as is reasonable (See contact info on Reverse Side)

NOTE: When reporting a suspected virus to your CSL or the CFP ensure that you record notes as needed on reverse side of this form and provide the technician with Your Name and Number.

CLASSIFIED MESSAGE INCIDENT (CMI) REPORTING PROCEDURES FOR USERS

A *CMI* is defined as a classified message that has been sent and/or received over an unclassified network or network of lower classification.

STEP 1	***STOP!*** **DISCONNECT LAN CABLE** *Discontinue use* of the system and **DO NOT** print the classified message unless directed to do so.
STEP 2	**SECURE** affected system(s) / printer(s), area / room. Limit the exposure of the CMI. **DO NOT** leave the system unsecured. Ensure all affected equipment remains under positive control of authorized personnel.
STEP 3	**TAKE NOTES** Apparent classification, Email Subject, file name, sender, date/time of msg, recipients. ***Mark your notes with the proper derivative classification***
STEP 4	**REPORT INCIDENT IMMEDIATELY** **DO NOT** discuss details of the CMI over unsecure lines. Call the CFP (See contact info on Reverse Side), your unit CSL, Supervisor and your Unit Security Manager

THE PHISHING THREAT IS REAL
STOP, THINK, before you CLICK

- No Airman is Entirely Safe from Phishing w/ targeted Social Engineering
- *Up to 80% of all malware attacks initiated through phishing attempts*
  - *-- Seeking PII, Access to Netwk, Operational Info, Delivery of Malware*
  - *-- Result: ID Theft, financial fraud, espionage, loss of Network/Data*

Three Steps of Phishing
- **The Lure - an enticement to give info/open a link or attachment**
- **The Hook - enticement prompts you to act, click the link/attach**
- **The Catch - info collected/malware planted/access gained**

Recognize Phishing Emails: (May contain these and/or other traits)
- Poses as Position of Authority/Expertise (Government or Commercial)
- Entices you to act now to avoid consequence or to gain reward
- Not from an individual and/or No Digital Signature
- Contains Grammatical Errors or Awkward/Uncommon Wording
- Web address link that shows a diff address when cursor is over link
- Improper/missing signature block or contact info
- Official/urgent email correspondence from gmail or similar service

Report Phishing:
- **DELETE** Suspicious Emails. May try to contact sender using contact info from other source (i.e. GAL) to validate email
- **REPORT** Reoccurring Phishing Emails. Use vESD link on desktop (Cyber Threat button) or Call CFP (See contact info on reverse)

June 2020

Prescribed by AFMAN 17-1301
Distribution: F

SEYMOURJOHNSONAFBVA33-200, 20210603

INFOCON LEVELS

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.
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.**

NETWORK USER "DOs & DONTs"

INTRODUCTION: All network users play a role in network integrity. 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, 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 24-hour force restart implementation.

For more information on Seymour Johnson AFB User information, refer to the 4th Communications Squadron SharePoint Page.
https://seymourjohnson.eim.acc.hedc.af.mil/4th_fw/MSG/cs/default.aspx

IMPORTANT POINTS OF CONTACT

Communications Focal Point (CFP): 722-2666 OPT. 2

Cybersecurity Office (WCO): 722-5028

Wing Information Protection (IP): 722-1454

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

Prescribed by AFMAN 17-1301
Distribution: F
SEYMOURJOHNSONAFBVA33-200, 20210603

INFOCON LEVELS

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.
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.**

NETWORK USER "DOs & DONTs"

INTRODUCTION: All network users play a role in network integrity. 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, 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 24-hour force restart implementation.

For more information on Seymour Johnson AFB User information, refer to the 4th Communications Squadron SharePoint Page.
https://seymourjohnson.eim.acc.hedc.af.mil/4th_fw/MSG/cs/default.aspx

IMPORTANT POINTS OF CONTACT

Communications Focal Point (CFP): 722-2666 OPT. 2

Cybersecurity Office (WCO): 722-5028

Wing Information Protection (IP): 722-1454

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

Prescribed by AFMAN 17-1301
Distribution: F
SEYMOURJOHNSONAFBVA33-200,20210603