

**Chapter XIII Computer Operations**

**Subject 3 Computer Virus**

**1303.01 Objective**

- A. To prevent the proliferation of Computer Viruses among Fire Division computers.

**1303.03 Procedures**

- A. All USB thumb drives and optical media must be checked for viruses or other malicious software (malware) before they are used. This may be done by launching a department approved antivirus application such as Symantec Endpoint. This is usually completed by “right-clicking” on the external target media and choosing the scan option if available. Other internet antivirus scanning tools may be used but only with Fire-IT administrator approval. If you have questions please contact your Fire-IT administrator for further instructions.
- B. If a virus or malware infection is suspected then a Fire-IT administrator must first be notified to prevent further out-break. All laptop and desktop computers should be scanned anytime viruses or malicious software is suspected. Please notify your Fire-IT administrator as soon as possible for further instructions.
- C. All files and applications downloaded from the internet/ intranet or other third-party department servers should be scanned for viruses before storage on any Fire Division computer. To do this, follow the instructions in item “A” above. If in doubt please contact your Fire-IT administrator for more instructions.