**Annexure-II**

**NSA and MHA**

## Conventional Cyber Security Norms and Best Practices

**A)** ***Do's and Don'ts to minimize malware (Virus, Trojan, and Worms etc.) infections while using Internet-connected or standalone Computers.***

**Do's**

1. Always use genuine software.
2. Install the latest updates/patches for Operating System, Antivirus and Application software.
3. Enable a firewall. Operating Systems have an inbuilt firewall which can be used to stop unwanted Internet connections.
4. Limit user privileges on the computer. Always access Internet as a standard user but not as Administrator.
5. Check and verify email sender IDs and web links before opening file attachments and clicking on links in emails and webpages.
6. Protect against social engineering attacks. Phishing emails and SMS are used to get user credentials like username, passwords, credit card and PIN numbers etc.
7. Regularly check the last logging details of email accounts.
8. Use strong passwords that include a combination of letters, numbers, and symbols.
9. Use only officially supplied USB storage media. USB storage media should be regularly formatted after use to erase any malicious files hidden from normal view.
10. Regularly take backup of document files to avoid loss of files in case of emergencies like malware infections, hard disk crash, corrupted applications and other unforeseen incidents.
11. Users should be periodically briefed about Cyber Security measures.

**Don'ts**

1. Avoid downloading and installing pirated software.
2. Internet-connected computers should not be used for drafting I storing sensitive official documents I correspondences.
3. Don't open emails from unknown email IDs. Such mails should be deleted from email account inbox.
4. Don't download and open file attachments that originated from unknown sources.
5. Auto storage of user name and password in browser /web page should be disabled in shared computers used for Internet activities.
6. Avoid using personal USB storage devices I Smart Devices on office
7. computers. Don't put unknown USB storage device into your Computer.
8. Don't share passwords with anyone. Don't use the same password on all websites and services.

**B) A few indicators of a Generic Malware infected computer:**

1. Computer runs slowly than normal, stops responding or freezes often. Computer crashes and restarts every few minutes.
2. Unusual error messages pop up constantly.
3. New toolbars, links, or favorites added to your web browser.
4. Home page, mouse pointer, or search program changes unexpectedly.
5. Unusual network traffic and connectivity from the computer even without doing any Internet activity.

(These are common signs of malware infection, but they may also be indicative of mere hardware or software problems.)

**C) *Tips to check and protect from malware infections in Windows computer.***

1. Always set automatic updates for Operating System, Anti-Virus and Applications. For Windows OS auto update can be done as follow: -

   **Control Panel-> Windows Updates-> Change Settings-> Install updates automatically.**

(For other software follow the steps as given in the respective software.)

2. Checking for unusual network traffic with Windows ***"netstat -na"*** command.

   **Type *"cmd"* in *"run"* and type *"netstat -na"*. Checkout foreign Established connection and IP addresses. Check the IP address for its ownership**

3. Check for any unusual executable running automatically at Windows startup.

   **Type *"msconfig"* in *"run"* and check for any unusual executable running automatically.**

   (Disable, delete or uninstall any unnecessary/unknown executable/ program.)

4. Enable hidden files, folders and system files view to find any unusual or hidden files, especially useful while using USB storage devises.

   **Control Panel -> Folder Options -> View -> select the "Show hidden files and folders" option and unselect "Hide protected operating system files"**

   Make sure there is no hidden file and folders present in the USB Storage device. Format the device if any unusual files (files having extensions exe, com, dat, scrand ini etc.) are present besides the data files (doc, ppt, xls and pdf etc.).

5. Delete the contents of Windows ***"Temp"*** and ***"Temporary Internet files"*** regularly.

   (a) Type **%temp%** in **"run"** and delete all the contents of temporary folder.

   (b) For deleting Temporary Internet Files follow steps as given by different browsers like Windows Internet Explorer, Google Chrome, Mozilla Firefox, Opera and Apple Safari.