INTERNET BROWSING SECURITY

1. While accessing Government applications/services, email services or banking/payment related services or any other important application/services, always use Private Browsing/incognito Mode in your browser.

2. While accessing sites where user login is required, always type the site's domain name/URL, manually on the browser's address bar, rather than clicking on any link.

3. Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches. Don't store any Usernames and passwords on the internet browser.

4. Don’t store any payment related information on the internet browser.

5. Don't use any 3rd part anonymization services (3rdparty VPN, Tor' proxies etc). Avoid using unauthorized VPN services and remote desktop tools like Anydesk and Teamviewer.

6. Don’t use any 3rd party toolbars (ex: download manager, weather tool bar, ask me tool bar etc.) in your internet browser.

7. Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software).

8. Don't use your official systems for installing or playing any Games.

9. Observe caution while opening any shortened URLs (ex: tinyurl.com/abS3fil). Many malwares and phishing sites abuse URL shortening services. Such links may lead to a phishing/malware webpage, which could compromise the device.

10. Cache and History should be deleted regularly from the browsers after every usage on internet connected systems.

11. Do not leave any official document on internet connected computers.

12. Enable genuine ad-blocker to protect from mal advertising.

13. Ensure the genuineness of SSL/TLS website while performing online transactions.

14. Use reputed browsers like Chrome, Edge, Firefox, etc.