Advisory and Resource Facilitation
National Informatics Centre.
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
IP No 5578
Csg-advisory@nic.in

NIC-CSG/2025-SPl/01
Dated: 10-05-2025

राष्ट्रीय सूचना विज्ञान केंद्र
National Informatics Centre

Annexure-1

Endpoint Security

1. Only endpoints with licensed Operation system (i.e., desktops, laptops, workstations) to be connected to the network.
2. All desktops shall be installed with Endpoint security solution such as Antivirus/EDR, UEM before connecting to NIC network.
3. All desktops / laptops USB ports shall be disabled. Only enabled after due approval of CISO
4. All network devices shall have MAC-binding done on network switches
5. Host Firewall to be enabled on all endpoints, restricting lateral movement within the same network segment.
6. Administrator privileges to be revoked for all the endpoints.
7. All endpoints connecting to the NIC network to be configured with a common NIC DNS and NTP server.
8. Every endpoint should have logging enabled and logs should be reviewed regularly.
9. Only approved softwares to be installed on systems.
10. Access to systems, servers, devices, including printers, scanners etc. to be protected with a password.
11. Sensitive files to be stored in encrypted form or password protected.
12. Use of Remote access tools to be prohibited within organization network.
13. All operating systems to be kept up to date with the latest security patches.
14. Mobile Device Management
    i. Mobile devices with sensory functions to be restricted within specified controlled zones where classified data is held.
    ii. Mobile phone features such as Wi-Fi, GPS, Bluetooth and NFC should be kept disabled by default and only activated when necessary or grant permission to Apps only if necessary.