NLC India Limited
(**“Navratna”** – A Government of India Enterprise)

Office of the Chief General Manager / Computer Services & ERP
Corporate Office
Telephone No.04142-212348 Fax No. 04142 - 252645 /252646

CIRCULAR

Cir No. CGM/CS/CybSecy_4/2024-6 Dt: 21.09.2024

Sub : Improving Cyber Security – Reg

In view of the evolving cyber threat landscape, it is essential to enforce access control policies for Internet, VPN & critical IT Systems like SAP. Accordingly, Internet usage policy of our Organization has been modified from blacklisting to whitelisting approach.

1) Internet Access has been provided from all desktops & laptops to websites/Internet Domains which are essential for performing business transactions like Government Web Sites (.gov.in), Video Conferencing sites (.lifesize.com, .vconsol.com, Microsoft teams) ,NIC websites (.nic.in), SRLDC, GeM, Income Tax/GST Portals etc., List of all such permitted websites is available in Intranet -> CAWL.

   If access to sites, which are not listed in CAWL section, is required for business transactions, request may be made, through E-Office, with Unit Head approval, to Corporate Computer Services for inclusion in the permitted websites list.

2) As per MeitY guidelines, Internet access through FTTH is restricted (Annexure-I).
3) Access to SAP is being provided from desktops which have been sanitized as per SoP (Annexure – II). SAP access from laptops will continue to be restricted till appropriate security measures are put in place.
4) Access to VPN is being provided to laptops of executives in the rank of Unit Head & above and their technical secretaries after ensuring compliance to SoP (Annexure-III) for the same.
   a) In addition to UserName /Password and OTP, authentication will be through Personal Digital Certificate issued from Corporate Computer Services..

   b) As VPN is used through Internet, additional security software will be installed in the laptop for pro-active monitoring of vulnerabilities and detection of security incidents in the laptop.

5) VPN & SAP access controls will be reviewed and modified, based on cyber security audit recommendations.

6) To facilitate hardening of desktops/laptops as per SoP, employees are requested to move user files (Word/Excel Documents , PDFs, Drawings, PPTs etc.,) outside C:Drive before hardening process can be taken up. License keys for reinstallation of Operating System and any other software shall be safely preserved by employees before reinstallation of Operating System .

7) In Windows systems, C: Drive is to be used for Operating System & Application Software. In situations of Windows Re-set/Re-Install, Hardware/Software failure, loss of user files/data in C: Drives is likely. To avoid such data loss, all employees are requested to save their files in drives other than C:\ such as D:, E: Drives.

8) Recently , two instances of employees installing unlicensed software in their official laptops and using the same from within NLCIL network have been brought to notice, leading to legal claims. Employees are not expected to use their official email id , NLCIL's network resources like Internet Gateway, Active Directory account etc., for purposes other than official usage. Employees should not install unauthorized software in their official laptops and any legal claim related to the same should be handled by the employee. NLCIL shall not be responsible for such legal claims and appropriate action can be initiated against such employee.

9) All employees are requested to comply to security guidelines communicated from time to time. Refer circulars under Intranet >> Corporate Computer Services >> Cybersecurity.

CGM/CCS&ERP

Copy

To All Executive Directors

All Heads of Units/Projects/JVs/Offices

All Group Heads of HR/Finance

All Unit HoHRs & Finance Heads

All Account Centers

Copy to:

TS/PS to CVO/FDs/CMD

ANNEXURE - I

1. SCOPE

The following guideline issued by National Informatics centre on Secure Local Area Network, Secure Wireless LAN, Desktop/Laptop Security and Server Security, shall be adhered to by the respective IT/Network teams of each Ministry/Department. The CISO of the Ministry/Department shall ensure the compliance of these guidelines.

2. SECURE LOCAL AREA NETWORK

2.1. Ensure that timely action is taken on the alerts and advisories issued by CERT-In and NIC-CERT.

2.2. All ICT devices should be connected via the Internet gateway of NIC's network (i.e. NICNET) and any other direct internet connection i.e., broadband, 3G/4G/5G etc., should be withdrawn with immediate effect. No hotspots to be used in the network

2.3. Ensure that an inventory of authorized hardware and software in the network is maintained.

2.4. Ensure that default credentials of network devices are changed.

2.5. Media Access Control (MAC) address binding or IEEE 802.1x is mandatory for all systems/IT devices connected in the Ministries/Department.

2.6. Unmanaged network devices should be replaced with managed devices on an immediate basis.

2.7. Ensure that organisation's or NIC DNS (IPv4: 1.10.10.10 / IPv6: 2409::1) server is configured for DNS.

2.8. Ensure that DNS queries for public DNS servers are not allowed in the network.

2.9. Ensure that NIC NTP (samay1.nic.in, samay2.nic.in) server is configured as NTP in the network.

2.10. Configure host firewall in all systems to restrict lateral traffic movement within the same network segments.

2.11. Internet connectivity to be withdrawn and Only NICNET connectivity to be provided to users who do not adhere to the guidelines mentioned under the head "*desktop/laptop and printer security*". Internet connectivity is to be restored with the approval of CISO of the ministry.

2.12. Network firewall shall be used to restrict traffic movement outside the network segment. Only selected ports and protocols shall be allowed for communication with selected IPs, as per the requirements of the official work.

2.13. Systems and equipment which are obsolete/unsupported/unpatched operating systems, to be removed from the network.

2.14. Ensure that Kavach Multi-Factor Authentication is configured on all the NIC Email Accounts in the Ministry.

2.15. It is recommended to have mechanism to identify unauthorized device and unauthorized software usage in the Network.

Annexure - II

SAP Access through Desktops

1) Check if two partitions are available – OS, UserFiles. Ensure separate partition for UserFiles

2) Scan UserFiles Partitions with Escan AV – D:, E: etc., (First AV Run)

3) Backup Existing Files – doc, docx, xls, xlsx, ppt, pptx, pdf, drawings etc.,

4) Retrieve Windows License Details

5) Format C: and install windows using clean image from Microsoft Site

6) Apply Windows License & Activate

7) Ensure proper entry for the system in Digital Assets application – update license details

8) Install AV, Restore backed up files, and scan full system with Escan AV (Second AV Run)

9) Configure Date/Time, Regional Settings

10) Set password for default 'Administrator' account and disable it. (Computer Management -> Local Users & Groups -> Users)

11) Create a new Local Administrator account 'admin', set password and keep it private. Do NOT share to users

12) Create a new normal user account 'nlc', set password and keep it private. Do NOT share to users

13) Ensure logon after pressing Ctrl + Alt + Del (Silent logon should NOT be enabled)
Local Security Policy -> Local Policies -> Security Settings -> Interactive Logon : Do not require Ctrl + Alt + Del -> Disable

14) Contact Network Admin and configure Bootp

15) Ensure IP address, DNS are assigned properly

16) Set Hostname.

17) Join PC to Domain. Use "auth_pcjoin" account for this operation.

18) Ensure FQDN of PC gets resolved correctly by DNS

19) Ensure AD Policies are applied – NTP, WSUS Server, Proxy Server

20) Ensure computer is created in proper OU in AD

21) Ensure Windows Defender Firewall & Anti-Virus are enabled

22) As Domain Admin, install/uninstall following software for all users

1) Uninstall Windows components – Solitaire & Casual Games, Xbox, Skype, News, Weather, One Drive, Films&TV, Maps, Feedback Hub etc.,

2) MS Office / Libre Office

3) Firefox / Chrome Browser

4) Adobe Acrobat Reader

5) SAP GUI

6) Printer Driver

23) Create bookmarks in browser for Intranet, Email, EOffice, AMS, Tel.Directory – Import from JSON file in firefox, HTML file n Chrome

24) Ensure switch port is configured for 802.1x authentication

25) Ensure Employee(s) can login to Active Directory Domain and access E-Office

26) Ensure Employees(s) can use the printer/scanner attached to the Desktop

The above SoP will be reviewed continuously and is subject to change.

Annexure - III

VPN Access through Laptops

(Locations where LAN/MPLS is available)

1) Check if two partitions are available – OS, UserFiles. Ensure separate partition for UserFiles
2) Scan UserFiles Partitions with Escan AV – D:, E: etc., (First AV Run)
3) Backup Existing Files – doc, docx, xls, xlsx, ppt, pptx, pdf, drawings etc.,
4) Retrieve Windows License Details
5) Format C: and install windows using clean image from Microsoft Site
6) Apply Windows License & Activate
7) Ensure proper entry for the system in Digital Assets application – update license details
8) Install AV, Restore backed up files, and scan full system with Escan AV (Second AV Run)
9) Configure Date/Time, Regional Settings
10) Set password for default 'Administrator' account and disable it. (Computer Management -> Local Users & Groups -> Users)
11) Create a new Local Administrator account 'admin', set password and keep it private. Do NOT share to users
12) Create a new normal user account 'nlc', set password and keep it private. Do NOT share to users
13) Ensure logon after pressing Ctrl + Alt + Del (Silent logon should NOT be enabled)
    Local Security Policy -> Local Policies -> Security Settings -> Interactive Logon : Do not require Ctrl + Alt + Del -> Disable
14) Contact Network Admin and configure Bootp
15) Ensure IP address, DNS are assigned properly
16) Set Hostname.
17) Join PC to Domain. Use "auth_pcjoin" account for this operation.
18) Ensure FQDN of PC gets resolved correctly by DNS
19) Ensure AD Policies are applied – NTP, WSUS Server, Proxy Server
20) Ensure computer is created in proper OU in AD
21) Ensure Windows Defender Firewall & Anti-Virus are enabled
22) As Domain Admin, install/uninstall following software for all users
    a) Uninstall Windows components – Solitaire & Casual Games, Xbox, Skype, News, Weather, One Drive, Films&TV, Maps, Feedback Hub etc.,
    b) MS Office / Libre Office
    c) Firefox / Chrome Browser