IT Security Restrictions

1. USB Usage:

Personal USB drives are not allowed. Only encrypted, IT-approved storage devices may be used.

2. VPN Policy:

Remote work requires VPN connection to access internal systems securely. Disabling VPN during work hours is prohibited.

3. Public Wi-Fi:

Avoid public networks. If unavoidable, use company VPN with DNS tunneling enabled.

4. Admin Access:

Only DevOps and authorized admin roles are granted elevated system permissions. Never run applications as administrator unless pre-approved.

5. Shared Terminals:

Always log out after each session. Auto-logout is configured for 10 minutes of inactivity.