

# Domain Server and Endpoint Security Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)  
Version: 1.0

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party

## Document Revision History:

Version	Date	Author	Changes Made	Reviewed By	Approved By
1	23/04/2024	Gyan Singh	Domain Server and Endpoint Security Policies and Procedures.	Mr.P.Sahoo	Mr.Amit Sobti

## 1. Purpose

To define the baseline IT security standards across all systems and users to protect company data, reduce security risks, and ensure compliance with client and operational standards.

## 2. Scope

Applies to:

- All domain-joined systems (desktops, laptops, servers)
- All employees, vendors, and third-party IT access
- All corporate locations including remote sites

### 3. Policy Statements

#### a. User Account & Authentication

- Unique domain credentials mandatory for all users.
- Enforced 2FA for all admins and webmail access.
- Password complexity: Minimum 12 characters with uppercase, lowercase, number, and symbol.
- Account lockout after 5 invalid login attempts.

#### b. Endpoint Device Restrictions

- **Snipping Tool, Snip & Sketch, and Windows + Shift + S screenshot shortcut** must be disabled via Group Policy.
- **Microsoft Store access** is blocked via GPO to prevent unauthorized app installations.
- **Incognito/Private Mode in Chrome and Firefox** is disabled via registry or GPO.
- **Microsoft Edge browser** is blocked or restricted to approved sites only.
- **Remote Desktop Connection (mstsc)** is disabled for all users except designated IT personnel.
- Drives (C:, D:, etc.) must be hidden or restricted via GPO for all end-users, unless otherwise approved.

#### c. Application & Admin Control

- Only approved software is allowed (AppLocker/SRP enforced).
- Users are not granted local admin rights.
- USB ports are disabled or read-only (except whitelisted systems).
- Blocking of executable files (.exe, .bat, .vbs) from unauthorized paths.

#### d. Network & System Configuration

- Windows Firewall must be enabled with enforced rules.
- Web access restricted via DNS/web filter (e.g., FortiGuard).

- Admin access to domain servers is secured with IP restriction and logging.
- No external VPN tools or file-sharing software allowed.

#### **e. Patch & Security Updates**

- Weekly patch cycle via WSUS or endpoint manager.
- Antivirus/EDR updates must auto-sync daily.
- Systems without recent updates are auto-isolated.

#### **f. Audit & Monitoring**

- Enable auditing for logon/logoff, file access, privilege changes.
- Logs are sent to a centralized SIEM or monitoring tool.
- USB, software installs, and policy violations must trigger alerts.

#### **g. Backups & Recovery**

- Domain controller backups are taken daily with encryption.
- System state and user data (shared drives) are backed up securely.
- Periodic restore tests are conducted.

#### **h. Incident Management**

- Report incidents to IT within 15 minutes of detection.
- IT team will investigate and respond within 24 hours.
- Documented post-incident reviews mandatory for critical events.

### **4. Enforcement**

Non-compliance may result in restricted access, disciplinary action, or termination depending on the severity.

### **5. Policy Review**

This policy will be reviewed bi-annually or upon major IT/operational changes.