**NexaCorp IT Support Manual**

**Section: IT Infrastructure Overview**

**Purpose:**  
To provide a comprehensive guide to NexaCorp’s IT support protocols, common technical issues, system maintenance, security procedures, and escalation workflows for diagnosing and resolving hardware, software, and network issues.

**Supported Tools & Systems:**

* Laptops & Desktops (Windows/macOS)
* VPN (NexaConnect)
* Shared Drives (P:\, G:\, Team Drives)
* Internal Portals (HRMS, Payroll, Asset Tracker)
* Official Email (Outlook with Exchange)
* Collaboration Tools (MS Teams, Zoom, Slack)
* Endpoint Protection (Trend Micro, Bitdefender)
* MDM (Mobile Device Management via Intune)
* Printer & Scanner Devices
* Asset Tracking System (NexaInvSys)

**Operational Hours:**

* IT Helpdesk: Monday to Friday, 9:00 AM – 7:00 PM IST
* Emergency Support: On-call for critical infrastructure issues (Ext. 2020)

**Section: Common IT Support Complaints & Resolutions**

**1. Cannot Connect to Shared Drive After Password Reset**

**Complaint:** “Post-password reset, I can't access the P:\Shared folder. It shows an authentication error.”

**Resolution Steps:**

* Instruct user to log off and log in with new credentials.
* Open Credential Manager > Windows Credentials > Remove any old domain entries.
* Open Command Prompt and clear cached credentials:  
  rundll32.exe keymgr.dll, KRShowKeyMgr
* Manually map network drive: \\fileserver\\shared
* If persistent, reset user permissions from AD Group Policy.

**Escalation:** Contact File Server Admin if issue persists beyond Level 1 support.

**2. VPN Error 720 / VPN Disconnects Randomly**

**Symptoms:** Repeated drops, error 720 or 619.

**Root Causes:**

* Corrupt WAN Miniport driver
* Conflicting adapters or IPv6

**Resolution Checklist:**

* Uninstall WAN Miniports using Device Manager > Network Adapters > Show Hidden Devices
* Restart system and reinstall VPN client (NexaConnect v5.4+)
* Disable IPv6 in Adapter settings > Properties
* Check firewall settings for IPsec tunnels

**Reference Document:** VPN\_TROUBLE\_GUIDE\_720.pdf

**3. Laptop Random Shutdowns After Windows Update**

**Symptoms:** Abrupt power-off without error; sometimes during idle.

**Diagnostics & Fixes:**

* Run battery diagnostics: powercfg /batteryreport
* Check Event Viewer > System > Look for Event ID 41 (Kernel-Power)
* BIOS update: Compare current version with OEM site
* Check CPU/GPU temperatures using HWMonitor
* Replace battery if wear level >40%

**4. Login Issues with HRMS or Portals**

**Issue:** “I’m unable to access HRMS or portal apps. Keeps redirecting or saying access denied.”

**Steps:**

* Confirm user account is active in Active Directory
* Unlock account if locked
* Clear SSO cookies (browser > advanced settings > cookies & site data)
* Try alternate browser
* Validate that SAML authentication is functional

**5. Screen Freezes or Black Screen at Boot**

**Scenarios:**

* System stuck on OEM logo
* No display output after boot

**Checklist:**

* Force shutdown and boot into Safe Mode (F8/Shift+Restart)
* sfc /scannow from CMD (admin)
* Disconnect all peripherals
* Reseat RAM (if under IT supervision)
* BIOS reset: Hold power + F2 (brand-specific)

**6. Slow System Performance Complaints**

**Symptoms:** Programs lag, unresponsive browser, slow boot.

**Troubleshooting:**

* Task Manager: Check CPU/Disk usage
* Disable startup apps (msconfig)
* Disk cleanup & defragmentation
* Scan with antivirus/malware tools
* Check RAM usage and consider upgrade

**7. Application Not Responding or Crashing**

**Steps:**

* Ensure latest version is installed
* Check for corrupted user profile (recreate temp profile)
* Look at Event Viewer logs > Application tab
* Check if app requires admin rights

**8. Printing/Scanning Not Working**

**Symptoms:** Printer shows offline or scan aborts.

**Actions:**

* Ensure device is connected to network
* Restart printer spooler: services.msc > Print Spooler > Restart
* Reinstall drivers from OEM site
* Test on alternate system to isolate user/device issue

**9. Outlook Fails to Send/Receive Email**

**Symptoms:** Stuck in outbox, sync issues.

**Steps:**

* Clear cache: File > Options > Mail > Empty Auto-Complete List
* Rebuild profile: Control Panel > Mail > Show Profiles > New
* Disable add-ins and restart in Safe Mode

**10. Audio or Webcam Not Working During Calls**

**Apps Affected:** Zoom, Teams, Webex

**Fixes:**

* Check device permissions in Windows Settings > Privacy > Camera/Mic
* Update drivers via Device Manager
* Test in Camera/Voice Recorder app
* Restart affected app and browser

**Section: Standard Operating Procedures (SOPs)**

**Laptop/Asset Allocation**

* Employee raises request via IT Asset Tracker portal
* Line manager approval mandatory
* IT dispatches device with pre-installed image
* Employee must digitally sign asset receipt form via HRMS
* Update Inventory Management Database (NexaInvSys)

**Password Reset & Account Unlock**

* Users can initiate reset via HRMS > Account Settings
* If account locked: Contact Helpdesk (Ext. 2020) to unlock via AD Console
* For VPN/Outlook sync issues, reconfigure credentials post-reset

**Email Configuration (Outlook)**

* Open Outlook → Auto-discover account
* Use company email and password
* Mobile setup via Microsoft Outlook app only
* Enforce 2FA for external email access

**New Software Installation**

* Raise request on Helpdesk portal with manager approval
* Check licensing requirements
* Install via SCCM or direct IT support

**Hardware Replacement SOP**

* Ticket raised by employee or detected during audit
* IT verifies issue, raises asset return request
* New hardware issued from approved asset pool
* Return form updated and signed

**Printer Configuration SOP**

* Add printer via IP: Control Panel > Devices > Add Printer > Add using TCP/IP
* Use driver based on printer model
* Test print page to confirm installation

**Mobile Device Management SOP**

* Enroll mobile device in Intune via Company Portal app
* Install mandatory work apps (Outlook, Teams)
* Configure email and passcode policies
* Remote wipe enabled for lost/stolen devices

**Section: Ticket Reporting & Escalation Workflow**

| **Issue Type** | **First Point of Contact** | **Escalation Level 2** | **SLA (Response)** |
| --- | --- | --- | --- |
| VPN / Remote Access | IT Helpdesk | Network Admin | 4 hrs |
| Drive Access | IT Helpdesk | File Server Admin | 4 hrs |
| System Hardware Fault | IT Desk | Asset Coordinator | 8 hrs |
| Email Issues | Email Admin | Exchange Server Admin | 4 hrs |
| Portal Access | Helpdesk | SSO/AD Admin | 2 hrs |
| Software Installation | IT Helpdesk | Endpoint Security Lead | 6 hrs |
| Mobile Device Issues | IT Helpdesk | Intune Admin | 6 hrs |
| Printing Issues | IT Helpdesk | Printer Coordinator | 4 hrs |

**Ticket Path:** Intranet > Helpdesk > Raise IT Ticket  
**Contact:** [itsupport@nexacorp.com](mailto:itsupport@nexacorp.com) | Ext: 2020

**Section: Security & Compliance**

* All company laptops must run Trend Micro Endpoint Security
* Unauthorized USB storage devices are blocked by default
* Phishing attempts must be reported to [phishing@nexacorp.com](mailto:phishing@nexacorp.com)
* Admin rights are restricted to IT team only
* Device encryption (BitLocker/macOS FileVault) is mandatory
* Monthly endpoint compliance audit conducted
* Data Loss Prevention (DLP) enabled on all client machines

**Security Policies:**

* ITSEC-02: System Access Policy
* VPNPOL-01: Remote Access Protocol
* ITSEC-07: Email Security & Threat Protection
* ITSEC-09: Patch Management Policy
* ITSEC-11: Mobile Device & BYOD Policy

**Section: Preventive Maintenance & Monitoring**

**Monthly Tasks:**

* Patch Windows via SCCM or WSUS
* Antivirus signature updates
* Disk health checks using CrystalDiskInfo
* Random system audits (5% assets/month)
* Password expiry reminders (per 90-day policy)
* Ensure printers are cleaned and operational

**Quarterly Tasks:**

* Port scanning and internal vulnerability testing
* Clean temporary cache/log files from devices
* Review logs from SIEM system for anomalies
* VPN configuration reviews for stale endpoints

**Annual Tasks:**

* Asset audit in coordination with Finance
* License compliance review
* Network penetration testing (by third-party)
* DR drill and recovery simulation (for critical systems)
* Employee awareness training on cybersecurity

**Appendix: Troubleshooting Cheat Sheet**

**VPN Error Codes:**

* 720: Protocol mismatch – reinstall client
* 619: Port blocked – reset firewall/router
* 800: No tunnel – check server status

**Common Boot Issues:**

* Black Screen: Check RAM/GPU
* Continuous Beeping: Memory or motherboard fault
* Blue Screen: Log minidump via Event Viewer > Analyze with WinDbg

**Quick Fixes:**

* Restart device
* Swap power adapter or cables
* Boot into Safe Mode + Diagnostic Tools

**Admin Tools:**

* SCCM Console
* AD Users & Computers
* Event Viewer
* PowerShell Scripts Library
* Remote Desktop / Intune

**Document Owner:** IT Operations  
**Version:** 3.2  
**Last Updated:** June 2025  
**Support Contact:** [itsupport@nexacorp.com](mailto:itsupport@nexacorp.com) | Ext: 2020