IT Helpdesk Agent Knowledge Base

This document provides comprehensive reference material for IT helpdesk agents assisting employees with technical issues. It includes standard procedures, troubleshooting advice, and compliance guidelines to ensure consistent and secure support across all departments.

1. Password Reset and Account Lockouts

When an employee forgets their password or gets locked out of their account, the helpdesk agent should first verify the user's identity using their employee ID and registered email address. Once verification is complete, the agent initiates a password reset using the Active Directory self-service portal or the appropriate API. If the account remains locked, the agent can confirm the status with the command "Get-ADUser -Identity <username> -Properties LockedOut" and unlock it using "Unlock-ADAccount -Identity <username>."
All password resets must be logged in the incident management system.

2. VPN Connection Troubleshooting

If a user cannot connect to the VPN, the agent should first confirm that they are using an approved corporate device with the correct VPN client, such as GlobalProtect or Cisco AnyConnect. The agent should ask the user to describe the error message and check whether the problem relates to invalid credentials or certificate errors. When the issue is certificate-related, the user should reinstall the VPN client from the Software Center. If the connection continues to fail, the agent should collect the VPN log files from the "C:\ProgramData\VPN\Logs\connection.log" directory and escalate the issue to the Network Team.

3. Email and Outlook Configuration

When setting up Outlook on a new or reimaged device, the agent should verify that the computer is domain-joined and that the user has an active mailbox. The agent can ask the user to run the "Test E-mail AutoConfiguration" option in Outlook by holding Control and right-clicking on the tray icon. If authentication fails, the user should clear stored credentials in Windows Credential Manager. For mobile devices, it is recommended to install the Microsoft Outlook app and sign in using corporate credentials.

4. Printer Installation and Troubleshooting

If a user reports that a printer is unavailable, the agent should confirm the printer name and check whether it appears under “Devices and Printers.” If not, the printer can be mapped manually using the path “\\printserver\\PRT-FLOOR3-02.” The agent should also confirm that the user has the necessary permissions in Active Directory to access that printer. Outdated drivers can cause printing errors, so the user should install the latest updates through Windows Update.

5. Software Installation and Access Policy

Helpdesk agents must ensure that employees install only approved software available in the Software Center. If a user requests software that is not listed, the agent must create a ticket in the ServiceNow system under “Software Access Request.” The user’s manager will review the business justification before IT Operations installs the software. Installation files must never be distributed via email or chat applications.

6. Remote Support and Quick Assist

When an employee needs direct help, the agent can provide remote assistance using Microsoft Quick Assist. The user should open Quick Assist and share the six-digit security code with the agent. The agent must not request any passwords or attempt to access confidential applications such as HR or finance systems. If the problem cannot be solved remotely, the agent should schedule an on-site session or escalate to the on-call engineer.

7. Network Connectivity Issues

If an employee experiences network issues, the agent should first determine whether the problem occurs on a wired or wireless connection. For wireless connections, the agent should verify that the user is connected to the corporate network “CorpNet” and that the device has a valid IP address. For wired connections, the agent should ask the user to check that the Ethernet cable is securely connected and the port LEDs are active. If the IP address begins with 169.x.x.x, this indicates a DHCP issue and the problem should be escalated to the Network Operations team.

8. Laptop Performance and Updates

When a user reports slow system performance, the agent should ask them to reboot the device and verify that sufficient disk space is available. The agent should confirm that

Windows updates have been installed and that no background processes are consuming excessive CPU resources. If the Microsoft Defender antivirus is scanning the system, the agent should advise the user to wait until the scan completes. Persistent issues may require escalation to Desktop Engineering for further diagnostics.

9. Two-Factor Authentication (2FA)

If a user cannot complete the two-factor authentication process, the agent should confirm whether they are using the Authenticator app or SMS verification. For Authenticator issues, the user can resync the app in the settings. For SMS verification, the agent should confirm that the phone number registered in the system is active. If access to the second factor is lost, the user must complete the identity verification procedure before resetting through the SecureID portal.

10. Policy Compliance and Security Awareness

All agents must adhere to the organization's IT security and compliance standards when assisting users. They should not disclose server names, credentials, or internal IP addresses. When a user reports a phishing email or suspicious attachment, the agent should instruct them to forward it to "phishing@company.local" and open a security incident ticket. Agents must remind users not to click on unknown links or download unverified files.