IT Helpdesk Guidelines

Section 3: Password Resets

Maintaining the security of your accounts is crucial. If you forget your password or need to reset it, follow the steps below to securely regain access to your account.

3.1 Using the Self-Service Password Reset (SSPR) Portal

Our organization provides a Self-Service Password Reset (SSPR) portal that allows you to reset your password without contacting the IT Help Desk.

Prerequisites:

- Ensure you are enrolled in the SSPR system. Enrollment involves setting up authentication methods (e.g., phone number, email) that will be used to verify your identity during the password reset process.

Steps to Reset Your Password:

1. **Access the SSPR Portal:**
    - Open a web browser and navigate to the SSPR portal at https://aka.ms/sspr.
2. **Enter Your User Information:**
    - In the provided field, enter your full company email address.
    - Complete the CAPTCHA verification as prompted to confirm you are not a robot.
    - Click **Next** to proceed.
3. **Select the Issue Type:**
    - Choose **"I forgot my password"** from the available options.
    - Click **Next**.
4. **Verify Your Identity:**
    - Select your preferred verification method from the options you configured during enrollment (e.g., text message, email).
    - Follow the on-screen instructions to complete the verification process. This may involve entering a code sent to your phone or email.
5. **Reset Your Password:**
    - Once your identity is verified, you will be prompted to create a new password. Ensure your new password meets the following complexity requirements:
        - At least 8 characters in length.
        - Includes at least one uppercase letter.
        - Includes at least one lowercase letter.
        - Includes at least one numeric digit.
        - Includes at least one special character (e.g., !, @, #, $).

    - Enter your new password in both the **"New password"** and **"Confirm new password"** fields.
    - Click **Next** to finalize the reset.
6. **Confirmation:**
    - A confirmation message will indicate that your password has been successfully reset.
    - You can now use your new password to log in to your account.

3.2 Best Practices for Password Security

To maintain the security of your account, adhere to the following best practices:

- **Create Strong Passwords:**
    - Use a combination of uppercase and lowercase letters, numbers, and special characters.
    - Avoid using easily guessable information such as birthdays, common words, or sequences (e.g., "password123" or "abcd1234").
- **Unique Passwords:**
    - Do not reuse passwords across multiple accounts. Each account should have a unique password to prevent a compromise of one account leading to others being compromised.
- **Regular Updates:**
    - Change your password periodically, at least every 90 days, to enhance security.
- **Use Multi-Factor Authentication (MFA):**
    - Whenever possible, enable MFA for an additional layer of security. This typically involves a second verification step, such as a code sent to your phone.
- **Secure Storage:**
    - Utilize a reputable password manager to securely store and manage your passwords. Avoid writing them down or storing them in unsecured documents.

3.3 Troubleshooting and Support

If you encounter any issues during the password reset process or have not enrolled in the SSPR system, please contact the IT Help Desk for assistance:

- **Email:** helpdesk@company.com
- **Phone:** (123) 456-7890
- **Hours of Operation:** Monday to Friday, 8:00 AM to 6:00 PM

By following these guidelines and utilizing the SSPR portal, you can efficiently manage your password resets and maintain the security of your account.

Section 4: Software Installation and Uninstallation

This section outlines the procedures for installing and uninstalling software on company-issued devices, ensuring compliance with organizational policies and maintaining system security.

4.1 Software Installation

Note: To maintain system integrity and security, employees are permitted to install only pre-approved software. All installations must adhere to the following procedures.

4.1.1 Installing Software via Software Center

The company provides a centralized platform, **Software Center**, for employees to access and install authorized software. This approach ensures that all applications are vetted and comply with organizational standards.

Steps to Install Software Using Software Center:

1. **Access Software Center:**
    - Click on the **Start** menu or press the Windows key.
    - Type **Software Center** in the search bar.
    - Select the **Software Center** application from the search results.
2. **Browse Available Applications:**
    - Upon launching Software Center, navigate to the **Applications** tab to view a list of software available for installation.
3. **Select and Install the Desired Application:**
    - Click on the desired software to view its details.
    - Click the **Install** button to initiate the installation.
    - Monitor the installation progress; once completed, the status will update to **Installed**.

Note: If the required software is not listed in Software Center, proceed to section 4.1.2.

4.1.2 Requesting Installation of Software Not Available in Software Center

If the desired software is not available in Software Center, employees must obtain approval from the IT department before proceeding.

Procedure:

1. **Submit a Software Installation Request:**
    - Complete the **Software Installation Request Form** available on the company intranet.
    - Provide detailed information, including:
        - Software name and version.
        - Purpose and justification for use.

        - Vendor or source of the software.
        - Any licensing requirements or costs.
2. **Await IT Department Approval:**
    - The IT department will review the request to ensure compatibility with existing systems and compliance with security policies.
    - Approval or denial will be communicated within [specified timeframe].
3. **Installation by Authorized Personnel:**
    - If approved, the IT department will coordinate the installation.
    - Employees are not permitted to install software from external sources independently.

Note: Unauthorized installation of software is strictly prohibited and may result in disciplinary action.

4.2 Software Uninstallation

To maintain system performance and security, unnecessary or outdated software should be uninstalled following the procedures below.

4.2.1 Uninstalling Software via Software Center

For applications installed through Software Center:

1. **Access Software Center:**
    - Open the **Start** menu.
    - Search for and select **Software Center**.
2. **Navigate to Installed Applications:**
    - Click on the **Installation Status** tab to view a list of installed applications.
3. **Select and Uninstall the Application:**
    - Click on the application you wish to uninstall.
    - Click the **Uninstall** button.
    - Confirm the uninstallation when prompted.

4.2.2 Uninstalling Software Not Listed in Software Center

For applications not managed through Software Center:

1. **Access Control Panel:**
    - Press **Windows + R**, type `appwiz.cpl`, and press Enter to open **Programs and Features**.
2. **Locate the Application:**
    - Scroll through the list to find the software to be uninstalled.
3. **Uninstall the Application:**
    - Right-click on the application and select **Uninstall**.
    - Follow the on-screen prompts to complete the process.

Note: If administrative privileges are required or if you encounter issues during uninstallation, contact the IT department for assistance.

4.3 Compliance and Enforcement

Adherence to these procedures ensures the security and efficiency of our IT infrastructure. Non-compliance may lead to security vulnerabilities and will be addressed according to company disciplinary policies.

For questions or further assistance, please contact the IT Help Desk at [contact information].

Section 5: Email Configuration

Proper configuration of your email client ensures seamless communication and adherence to company standards. This section provides detailed instructions for setting up your email account on various platforms.

5.1 Configuring Email on Microsoft Outlook

Prerequisites:

- Your full company email address and password.
- Incoming and outgoing mail server details provided by the IT department.

Steps:

1. **Open Microsoft Outlook:**
    - Launch the Outlook application on your device.
2. **Add a New Account:**
    - Navigate to **File** > **Add Account**.
3. **Enter Email Details:**
    - Select **Manual setup or additional server types** and click **Next**.
    - Choose **POP or IMAP** and click **Next**.
    - Fill in the following fields:
        - **Your Name:** Enter your full name.
        - **Email Address:** Enter your full company email address.
        - **Account Type:** Select **IMAP**.
        - **Incoming Mail Server:** Enter the IMAP server address provided by IT.
        - **Outgoing Mail Server (SMTP):** Enter the SMTP server address provided by IT.
        - **User Name:** Enter your full company email address.
        - **Password:** Enter your email password.
4. **Test Account Settings:**
    - Click **Test Account Settings** to verify connectivity.

- If tests are successful, click **Next** and then **Finish**.

5.2 Configuring Email on Mobile Devices

For iOS (iPhone/iPad):

1. **Open Settings:**
   - Tap the **Settings** app.
2. **Add Account:**
   - Scroll down and tap **Mail** > **Accounts** > **Add Account**.
3. **Enter Email Details:**
   - Select **Other** > **Add Mail Account**.
   - Fill in the following fields:
     - **Name:** Enter your full name.
     - **Email:** Enter your full company email address.
     - **Password:** Enter your email password.
     - **Description:** Enter a description (e.g., "Work Email").
   - Tap **Next**.
4. **Configure Servers:**
   - Under **Incoming Mail Server**, enter:
     - **Host Name:** Enter the IMAP server address provided by IT.
     - **User Name:** Enter your full company email address.
     - **Password:** Enter your email password.
   - Under **Outgoing Mail Server**, enter:
     - **Host Name:** Enter the SMTP server address provided by IT.
     - **User Name:** Enter your full company email address.
     - **Password:** Enter your email password.
5. **Save Settings:**
   - Tap **Save** to complete the setup.

For Android:

1. **Open Settings:**
   - Tap the **Settings** app.
2. **Add Account:**
   - Scroll down and tap **Accounts** > **Add Account** > **Email**.
3. **Enter Email Details:**
   - Enter your full company email address and tap **Manual Setup**.
   - Select **IMAP**.
   - Fill in the following fields:
     - **Username:** Enter your full company email address.
     - **Password:** Enter your email password.
     - **IMAP Server:** Enter the IMAP server address provided by IT.
     - **Port:** Enter the IMAP port number (typically 993 for SSL).
     - **Security Type:** Select **SSL/TLS**.
     - **SMTP Server:** Enter the SMTP server address provided by IT.

        - **Port:** Enter the SMTP port number (typically 465 or 587).
        - **Security Type:** Select **SSL/TLS**.
        - **Require Sign-In:** Ensure this is checked.
4. **Complete Setup:**
    - Tap **Done** to finish the configuration.

5.3 Configuring Email on Web Browsers

Accessing your email through a web browser ensures you can check your messages from any location without configuring an email client.

1. **Open Web Browser:**
    - Launch your preferred web browser (e.g., Chrome, Firefox, Edge).
2. **Navigate to Webmail:**
    - Enter the webmail URL provided by the IT department (e.g., https://webmail.company.com) in the address bar and press Enter.
3. **Log In:**
    - Enter your full company email address and password.
    - Click **Log In** to access your email account.

5.4 Best Practices for Email Security

- **Use Strong Passwords:**
    - Create complex passwords combining letters, numbers, and special characters.

Section 6: Handling Internet Connectivity Issues

Reliable internet access is essential for daily operations. If you experience connectivity problems, follow the steps below to diagnose and resolve common issues.

6.1 Preliminary Checks

1. **Verify Network Connection:**
    - Ensure your device is connected to the correct Wi-Fi network or via Ethernet.
    - Check for physical disconnections or loose cables.
2. **Check Airplane Mode:**
    - Confirm that Airplane Mode is turned off:
        - On Windows:
            - Navigate to **Settings** > **Network & Internet** > **Airplane mode**.
            - Ensure Airplane mode is set to **Off**.
        - On macOS:
            - Click the **Wi-Fi** icon in the menu bar.
            - Ensure **Airplane Mode** is not enabled.
3. **Restart Your Device:**

- Rebooting can resolve temporary software glitches affecting connectivity.

6.2 Modem and Router Troubleshooting

1. **Restart Modem and Router:**
   - Unplug the power cords from both devices.
   - Wait at least 30 seconds.
   - Plug in the modem first; wait for it to fully boot up (indicated by stable lights).
   - Plug in the router; wait for it to fully boot up.
   - This process can resolve many connectivity issues by refreshing the connection to your Internet Service Provider (ISP). cite turn0search0
2. **Check Modem and Router Lights:**
   - Refer to the device manuals to interpret indicator lights.
   - Ensure all necessary lights are lit, indicating proper operation.
3. **Inspect Cables and Connections:**
   - Verify that all cables are securely connected and undamaged.
   - Replace any frayed or damaged cables.

6.3 Device-Specific Troubleshooting

1. **For Windows Devices:**
   - **Release and Renew IP Address:**
     - Open **Command Prompt** as an administrator:
       - Press `Windows Key + X` and select **Command Prompt (Admin)**.
     - Type `ipconfig /release` and press Enter.
     - Type `ipconfig /renew` and press Enter.
   - **Flush DNS Cache:**
     - In Command Prompt, type `ipconfig /flushdns` and press Enter.
   - **Check IP Configuration:**
     - Ensure your device is set to obtain an IP address automatically:
       - Go to **Control Panel** > **Network and Sharing Center** > **Change adapter settings**.
       - Right-click your active network adapter and select **Properties**.
       - Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
       - Ensure both options are set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**. cite turn0search6
2. **For macOS Devices:**
   - **Renew DHCP Lease:**
     - Go to **System Preferences** > **Network**.
     - Select your active network connection.
     - Click **Advanced**, then the **TCP/IP** tab.
     - Click **Renew DHCP Lease**.
   - **Verify DNS Settings:**
     - In the same **Advanced** window, go to the **DNS** tab.
     - Ensure valid DNS servers are listed.

6.4 Advanced Troubleshooting

1. **Check for Interference:**
    - Ensure your router is placed away from devices that can cause interference, such as microwaves and cordless phones.
    - Keep the router elevated and centrally located for optimal coverage.
2. **Update Network Drivers:**
    - Ensure your network adapter drivers are up to date.
    - Visit the manufacturer's website to download the latest drivers.
3. **Run Network Diagnostics:**
    - Use built-in network diagnostic tools:
        - On Windows:
            - Right-click the network icon in the taskbar and select **Troubleshoot problems**.
        - On macOS:
            - Use the **Network Diagnostics** tool when prompted.
4. **Check for Malware:**
    - Run a full system scan using your antivirus software to rule out malware affecting connectivity.
5. **Bypass Router:**
    - Connect your device directly to the modem using an Ethernet cable.
    - If the connection works, the router may be malfunctioning.

6.5 Contacting IT Support

If you've completed the above steps and still experience connectivity issues:

- **Gather Information:**
    - Note any error messages received.
    - Document the steps you've already taken to troubleshoot.
- **Contact IT Support:**
    - Submit a detailed support ticket through the company's IT support portal.
    - Include all gathered information to assist in diagnosing the issue.

Timely reporting of persistent connectivity issues helps maintain productivity and allows IT support to address potential network-wide concerns.

Section 7: Resolving VPN Connectivity Issues

A Virtual Private Network (VPN) is essential for secure remote access to company resources. If you experience VPN connectivity issues, follow the detailed steps below to diagnose and resolve common problems.

7.1 Preliminary Checks

1. **Verify Internet Connection:**
    - **For Windows:**
        - Click on the **Network** icon in the taskbar.
        - Ensure you are connected to the correct network.
        - Open a web browser and navigate to a website to confirm internet access.
    - **For macOS:**
        - Click on the **Wi-Fi** icon in the menu bar.
        - Verify you are connected to the appropriate network.
        - Open Safari or another browser to check internet connectivity.
2. **Confirm VPN Credentials:**
    - Ensure your username and password are correct.
    - Check for any recent password changes or account lockouts.
3. **Restart VPN Application and Device:**
    - **Restart VPN Application:**
        - Close the VPN application completely.
        - Reopen the application and attempt to connect again.
    - **Restart Device:**
        - **For Windows:**
            - Click on the **Start** menu.
            - Select **Restart** and wait for the system to reboot.
        - **For macOS:**
            - Click on the **Apple** menu.
            - Select **Restart** and confirm.

7.2 Advanced Troubleshooting Steps

1. **Test VPN Server Reachability:**
    - **Ping Test:**
        - Open **Command Prompt** (Windows) or **Terminal** (macOS).
        - Type `ping [VPN server address]` and press Enter.
        - Replace `[VPN server address]` with your organization's VPN server address.
        - If you receive replies, the server is reachable. If not, there may be a network issue.
    - **Traceroute Test:**
        - In **Command Prompt** or **Terminal**, type `tracert [VPN server address]` (Windows) or `traceroute [VPN server address]` (macOS) and press Enter.
        - This will display the path your connection takes to reach the VPN server, helping identify where the connection fails.
2. **Review VPN Client Logs:**
    - **For OpenVPN:**
        - **Windows:**
            - Navigate to `C:\Users\<Username>\AppData\Roaming\OpenVPN Connect\log`.
            - Open `ovpn.log` with a text editor.

        - **macOS:**
            - Logs are typically stored in `/var/log/syslog`.
            - Use the `Console` application to view logs.
    - **For FortiClient:**
        - **Windows:**
            - Logs are located in `C:\Program Files\Fortinet\FortiClient\logs\trace` and `C:\Users\<Username>\AppData\Roaming\FortiClient\logs\trace`.
            - Review logs for errors.
    - **For Azure VPN Client:**
        - Click the arrows icon at the bottom-right corner of the Azure VPN Client window to show the Status Logs.
        - Check the logs for errors that might indicate the problem.
    - **For Cisco AnyConnect:**
        - Navigate to **Advanced Window** > **Statistics** > **VPN**.
        - Review the logs for any issues.
    - Error messages are typically displayed in red and can guide you to specific issues.
3. **Check Network Configuration:**
    - **Firewall and Antivirus Settings:**
        - Ensure that your firewall or antivirus software is not blocking the VPN connection.
        - Temporarily disable them and attempt to connect. If successful, adjust the settings to allow VPN traffic.
    - **Router Settings:**
        - Access your router's web interface:
            - Open a web browser.
            - Enter the router's IP address (commonly `192.168.1.1`) in the address bar.
            - Log in with your administrator credentials.
        - **Enable VPN Passthrough:**
            - Navigate to the **VPN** or **Security** section.
            - Locate the VPN Passthrough settings.
            - Ensure that the appropriate passthrough options (e.g., IPSec, PPTP, L2TP) are enabled.
            - Save changes and reboot the router if necessary.
        - **Note:** Modern VPN protocols like OpenVPN, IKEv2, and WireGuard are generally compatible with NAT and may not require VPN passthrough.
4. **Update VPN Client Software:**
    - Ensure you are using the latest version of the VPN client:
        - Visit the official website of your VPN provider.
        - Download and install the latest version.
        - Reattempt the VPN connection after updating.
5. **Disable Conflicting Software:**
    - Temporarily disable other VPN clients or security software that might interfere with the connection.

Section 10: Accessing IT Support Services for Complex Data Recovery Issues

In the event of complex data loss scenarios, it is imperative to engage with IT support services equipped with specialized expertise and tools to recover critical information. This section provides detailed instructions on how to access our IT support services for complex data recovery issues.Secure Data Recovery+1Downtown Computers+1

10.1 Recognizing the Need for Professional Data Recovery Services

Complex data recovery situations may include:

- Physical damage to storage devices (e.g., hard drives with mechanical failures).
- Logical errors resulting in inaccessible or corrupted data.
- Data loss due to malware attacks or system crashes.
- Failure of RAID arrays or other advanced storage configurations.

If you encounter such issues, it is advisable to seek professional assistance promptly to maximize the chances of successful data recovery.

10.2 Initiating Contact with IT Support for Data Recovery Assistance

1. **Gather Essential Information:**
    - Document the nature of the data loss, including any error messages or unusual system behaviors observed.
    - Note the make, model, and specifications of the affected storage device.
    - Compile a list of critical files or data types that require recovery.
2. **Contact IT Support:**
    - **Phone Support:**
        - Call our dedicated IT support hotline at [Insert Phone Number].
        - Provide the gathered information to the support representative.
        - Follow any preliminary troubleshooting steps suggested.
    - **Email Support:**
        - Send an email to [Insert Support Email Address] with the subject line "Data Recovery Assistance Request."
        - Include all relevant information and a detailed description of the issue.
        - Attach any error logs or screenshots, if available.
    - **Online Support Portal:**
        - Visit our IT support portal at [Insert URL].
        - Complete the data recovery assistance request form with accurate details.
        - Submit the form and monitor your email for updates.
3. **Schedule an Assessment:**
    - Our IT support team will contact you to schedule a convenient time for an in-depth assessment of the data loss situation.Secure Data Recovery
    - During the assessment, a technician will:

- Evaluate the extent of data loss and identify potential recovery methods.
- Discuss the feasibility of recovery and provide an estimated timeline.
- Offer a cost estimate for the data recovery service