General guidelines for categorising requests as assessing Priority.

Categorize the incident accurately based on predefined categories.

1. Password and Account Management:

   Examples:

- Password Resets: Assisting users who have forgotten their passwords or need to reset them due to security reasons.
- Account Creations: Creating new user accounts for employees or clients, granting access to various systems and services.
- Username Recovery: Helping users retrieve their forgotten usernames or login IDs.

2. Software and Application Support

   Examples:

- Providing guidance and troubleshooting assistance during the installation of software applications on users' devices.
- Software Installation
- Application Errors: Resolving issues related to errors or crashes that occur while using specific software applications.
- Configuration Assistance: Helping users configure software settings according to their requirements or fixing misconfigurations.

3. Hardware Troubleshooting:

   Examples:

   Desktop Issues: Addressing problems with desktop computers, such as boot failures, hardware malfunctions, or abnormal behavior.

- Laptop Troubles: Assisting users with laptop-related problems, like battery issues, display problems, or keyboard malfunctions.
- Printer and Peripheral Support: Troubleshooting and resolving issues with printers, scanners, keyboards, mice, and other peripherals.

4. Network Connectivity:

- Examples:
- Wi-Fi Problems: Diagnosing and resolving issues with wireless network connections and Wi-Fi access points.

- Internet Access Issues: Troubleshooting problems that prevent users from accessing the internet due to network or connectivity problems.
- Network Connectivity Problems: Assisting with general network connectivity issues, like network card configuration or DNS problems.

5. Email and Communication:

   Examples:

- Email Setup: Assisting users with configuring email accounts on various email clients or devices.
- Email Access Issues: Addressing problems related to accessing email accounts, login errors, or syncing issues.
- Email Errors: Resolving issues with error messages or problems encountered while sending, receiving, or managing emails.

6. Security and Access Control:

   Examples:

- Access Requests: Handling requests from users for access to specific resources, applications, or network folders.
- Permissions Management: Managing user permissions and access rights to ensure data security and adherence to company policies.
- Security Inquiries: Addressing user concerns or questions about security practices, policies, or potential security threats.

7. General IT Inquiries:

   Examples:

- Non-Specific IT Queries: Answering general questions about IT services, hardware, software, or technology-related topics.
- Technology Advice: Providing guidance and recommendations on IT solutions, best practices, or suitable tools for specific needs.

Prioritize incidents based on impact and urgency to ensure timely resolution.

1. Priority Level: Low

- Description: Incidents categorized as "Low" priority are non-critical and have a minimal impact on the user's ability to work. These incidents usually involve general inquiries, informational requests, or minor issues that do not significantly impact business operations.
- Example: Request for software installation on a user's workstation, a password reset for an account with no immediate work impact, or assistance with updating personal information in the system.

2. Priority Level: Medium

- Description: Incidents categorized as "Medium" priority have a noticeable impact on the user's ability to work but do not cause critical disruptions. These incidents might involve issues that impact individual productivity or specific tasks, but there are workarounds available.
- Example: Inability to access a shared network folder required for a project, a software application crashing intermittently, or a printer not functioning for a team that relies on hard copies for meetings.

3. Priority Level: High

- Description: Incidents categorized as "High" priority are critical and have a severe impact on the user's ability to perform essential tasks. These incidents usually result in a significant disruption of work for the affected individual or team and require immediate attention.
- Example: Complete network outage preventing all users from accessing critical systems, a server malfunction affecting multiple users' access to essential data, or an email service outage preventing communication for the entire organization.
- Remember, the priority levels may vary based on the organization's policies and the nature of the incident. It's important to have well-defined criteria for determining the priority of incidents so that the Service Desk team can effectively allocate resources and provide timely support.

Frequently Asked Questions:

1) **Q: How do I reset my password?**

A: Go to “Where to Reset my Password for which application” web page @ the following link – www.anycorp.intranet.passwordreset/com. There you will be able to select application for which you need to reset your password and will receive further instructions.

2) **Q: My internet connection is not working. Can you help me troubleshoot it?**

A: Please follow below steps:

1) Check physical connections:
- Ensure that all cables (Ethernet, modem, router, etc.) are securely connected.
- Power cycle your modem and router by unplugging them from the power source, waiting for 30 seconds, and then plugging them back in.

2) Verify Wi-Fi settings (for wireless connections):
- Make sure the Wi-Fi on your device is turned on.
- Check if you are connected to the correct Wi-Fi network.
- Try disconnecting and reconnecting to the Wi-Fi network.

3) Test connectivity on other devices:
- Check if other devices (e.g., smartphones, tablets, other computers) can connect to the internet. This helps determine if the issue is specific to your device or a broader network problem.

4) Restart your device:
- Restart your computer or device to refresh network settings.

5) Disable/enable network adapters:
- For Windows: Go to the Control Panel > Network and Internet > Network and Sharing Center. Click on "Change adapter settings" on the left-hand side. Right-click on the active network adapter and select "Disable." After a few seconds, right-click again and select "Enable."
- For Mac: Go to System Preferences > Network. Select the active network connection on the left-hand side and click the minus (-) button to remove it. Then click the plus (+) button and re-add the network connection.

3) **Q: How do I connect to Any Corp's Corporate Wi-Fi network?**

A: 1. Go to your device's Wi-Fi settings.

- For Windows: Click on the Wi-Fi icon in the system tray at the bottom right corner of the screen, then click "Network & Internet settings" and select "Wi-Fi" from the left-hand menu.
- For Mac: Click on the Wi-Fi icon in the menu bar at the top right corner of the screen.
- For iOS (iPhone/iPad): Go to "Settings" > "Wi-Fi."
- For Android: Go to "Settings" > "Network & internet" > "Wi-Fi."

2. Look for the available Wi-Fi networks.

   • Locate the list of available Wi-Fi networks. It may be labelled as "Any Available Networks" or "Choose a Network."

3. Select Any Corp's corporate Wi-Fi network.

   • Look for the network name (SSID) that corresponds to your corporate Wi-Fi network.

   • When you firstly joined Any Corp, an email was sent to you with a list of all Any Corp's Corporate Office and Wi-Fi password, find that email and check which Any Corp Location you are in and use the provided credentials

   • If you can't locate the email then a colleague can logon Any Corp's Intranet and under Any Corp's Office Locations > Go to Wi-Fi details or if you still need help, contact IT Helpdesk

   • Click or tap on the network name to select it.

4. Enter the Wi-Fi network password.

   • If prompted, enter the Wi-Fi network password or security key.

5. Verify the connection.

   • Once you've entered the password, your device will attempt to connect to the corporate Wi-Fi network.

   • Wait for a moment until your device confirms the successful connection. You should see a connected status or Wi-Fi icon on your device's screen.

6. Test the internet connection.

   • Open a web browser or any internet-dependent application to ensure that you have successfully connected to the internet through the corporate Wi-Fi network.

   • Visit a website or perform a network-dependent task to verify the connectivity.

   • If you have successfully performed all the tasks above and your Wi-Fi still doesn't work, then please contact IT Helpdesk

4) Q: I accidentally deleted a file. Can it be recovered?

A:

1. Check the Recycle Bin or Trash:

   • Windows: Open the Recycle Bin by double-clicking its icon on the desktop. Locate the deleted file, right-click on it, and select "Restore" to return it to its original location.

   • Mac: Open the Trash by clicking on its icon in the Dock. Find the deleted file, right-click on it, and choose "Put Back" to restore it to its original location.

2. Use File History or Time Machine (for backups):

   - Windows: If you have enabled File History or created a backup using third-party software, you can restore the deleted file from your backup.

   - Mac: If you have enabled Time Machine and regularly backed up your files, you can enter Time Machine, locate the file at an earlier point in time, and restore it.

3. Search for temporary or hidden copies:

   - Some applications or the operating system itself may create temporary or hidden copies of files. Use the search functionality on your computer to search for the file by its name or extension. Look for any temporary or hidden folders that might contain a copy of the deleted file.

4. Contact IT Helpdesk

   - If the above methods don't recover the file and the file is deemed business critical, then please contact the IT Helpdesk and if a business case can be made for deploying data recovery software to help.

5) Q: My computer is running slow. Is there anything I can do to improve its performance?

A:

Yes, try the following hints and tips:

1. Restart your computer:

   - Sometimes, a simple restart can resolve temporary performance issues by clearing out system resources and processes.

2. Check for malware and viruses:

   - Run a full scan with your antivirus software to check for any malware or viruses that may be slowing down your computer. If any threats are detected, follow the recommended actions to remove them.

3. Free up disk space:

   - Delete unnecessary files and programs to free up disk space. Use the built-in Disk Cleanup tool on Windows or manually remove files and applications you no longer need.

4. Manage startup programs:

   - Reduce the number of programs that automatically start when your computer boots up. Open the Task Manager (Ctrl+Shift+Esc on Windows) and go to the "Startup" tab. Disable any unnecessary programs from starting up.

5. Disable visual effects:

- Adjusting visual effects can improve performance. On Windows, right-click on "This PC" or "My Computer," select "Properties," then go to "Advanced system settings." Under the "Performance" section, click on "Settings" and choose "Adjust for best performance" or manually disable specific visual effects.

6. Update software and drivers:

   - Ensure that your operating system, drivers, and software are up to date. Updates often include bug fixes and performance improvements.

7. Increase virtual memory:

   - Adjusting virtual memory (also known as the page file) can help improve performance. On Windows, go to "Advanced system settings" (follow step 5), click on the "Advanced" tab, and under the "Performance" section, click on "Settings." Go to the "Advanced" tab again and click on "Change" under Virtual Memory. Adjust the settings based on your system's specifications or let Windows manage it automatically.

8. Upgrade hardware components:

   - If your computer continues to run slowly after performing the above steps, consider upgrading hardware components such as adding more RAM or replacing the hard drive with a solid-state drive (SSD). Consult with a professional or refer to your computer's documentation for compatibility and installation instructions.

9. Regularly maintain your computer:

   - Perform regular disk cleanup, disk defragmentation (if using a traditional hard drive), and system maintenance tasks. These tasks can optimize performance and improve overall stability.

6) Q: How do I install a software application?

A:

1. Any Corp does not permit the installation of software applications without prior approval.

2. Please check Any Corp’s Intranet page > Approved Software Catalogue

3. Find the software you wish to install and follow the instructions in the read.me which downloads automatically with the installation file

4. If you can’t find the software in the Catalogue, please contact the IT Helpdesk

Q: I can't print. What should I check or do to fix the issue?

1. Check printer connections:

- Ensure that your printer is properly connected to your laptop via USB, network, or wireless connection. Make sure all cables are securely connected.

2. Confirm printer power and status:

   - Check that your printer is turned on and has no error messages or warning lights indicating an issue. If necessary, refer to the printer's manual for troubleshooting steps.

3. Set printer as default:

   - On your laptop, go to the "Control Panel" (Windows) or "System Preferences" (Mac) and navigate to the "Printers" or "Print & Scan" section. Right-click on your printer and select "Set as default printer" (Windows) or click the lock icon and enter your password, then select your printer and click the "Set as default" button (Mac).

4. Clear print queue:

   - Sometimes, print jobs can get stuck in the print queue and cause issues. Open the print queue by clicking on the printer icon in the system tray (Windows) or the printer settings (Mac). Cancel any pending print jobs, and then try printing again.

5. Restart printer and laptop:

   - Power off your printer and laptop completely. Wait for a few seconds, then power them back on. This can resolve temporary issues and refresh the printer and computer connections.

6. Update printer drivers:

   - Outdated or incompatible printer drivers can cause printing problems. Visit the printer manufacturer's website and search for the latest drivers for your specific printer model. Download and install the updated drivers on your laptop.

7. Check printer settings:

   - Open the printer properties or settings on your laptop. Ensure that the correct printer is selected and verify that the settings (such as paper size, print quality, etc.) match your desired print job.

8. Test with a different document or application:

   - Try printing from a different document or application to see if the issue is specific to one file or program. If you can print successfully from other sources, the problem may lie within the original document or application.

9. Restart print spooler service (Windows):

   - Open the "Services" application on your laptop. Locate the "Print Spooler" service, right-click on it, and select "Restart." This action clears the print spooler and can resolve certain printing issues.

10. Reinstall printer software:

- If all else fails, uninstall the printer software from your laptop and reinstall it. Visit the printer manufacturer's website and download the latest software for your printer model. Follow the provided instructions to reinstall the printer on your laptop.

7) Q: How do I access shared network drives?

A:

1) Ensure Network Connectivity:
   - Make sure your computer is connected to the network, either via Ethernet cable or Wi-Fi.

2) Know the Shared Drive Path:
   - You should have the network path or UNC (Universal Naming Convention) of the shared drive. It typically looks like this: \\computername\sharename or \\IP_address\sharename.

3) Open File Explorer:
   - Open File Explorer (Windows Explorer) on your computer.

4) Map a Network Drive (Optional):
   - If you want to access the shared drive frequently, you can map it as a network drive:

5) In File Explorer, go to "This PC."
   - Click on "Computer" in the top menu and select "Map network drive."
   - Choose a drive letter and enter the UNC path (e.g., \\server\share).
   - Check the box that says "Reconnect at sign-in" if you want it to be available every time you log in.
   - Click "Finish."

6) Access the Shared Drive:
   - If you've mapped the drive, you can find it under "This PC" with the assigned drive letter.
   - If you haven't mapped the drive, you can directly access it by entering the UNC path in the address bar of File Explorer and pressing Enter.

7) Provide Credentials (if required):
   - If the shared drive requires authentication, a window may pop up asking for a username and password. Enter your credentials, and check "Remember my credentials" if you want to avoid entering them every time.

8) Access Files and Folders:
    - Once you're connected to the shared drive, you can browse, open, and manage files and folders just like you would on your local drive.

Please note that the exact steps may vary depending on your network configuration and the version of Windows you are using. Additionally, you'll need appropriate permissions and credentials to access the shared drive.

8) Q: My computer is infected with malware. What steps should I take to remove it?

A:

1) Isolate the infected computer:
    - Disconnect from the internet to prevent the malware from communicating with its command and control servers.
    - Disconnect any external storage devices, such as USB drives, to prevent further infection.
2) Identify the malware:
    - Use reputable antivirus or anti-malware software to scan your computer and identify the malware. If you don't have one installed, consider downloading and installing a trusted antivirus program.
3) Remove the malware:
    - Follow the instructions provided by your antivirus software to remove the detected malware. This often involves quarantining or deleting infected files and cleaning your system.
4) Update your operating system and software:
    - Make sure your operating system and all installed software are up to date. Malware often takes advantage of vulnerabilities in outdated software.
5) Change passwords:
    - If you suspect that the malware has access to your sensitive information, change your passwords for important accounts, such as email, online banking, and social media.
6) Restore or reinstall the operating system (if necessary):
    - In severe cases, you may need to reinstall your operating system to ensure complete removal of the malware. Make sure to back up your important data before doing this.
7) Install preventive measures:
    - After removing the malware, install reputable antivirus software and keep it updated to help prevent future infections. Also, enable your computer's built-in firewall.

9) Q. How do I connect to the Any Corp's Corporate VPN (Virtual Private Network)?

A:

1) Obtain VPN Credentials:

- Your company's IT department will provide you with the necessary credentials for connecting to the VPN. This typically includes a username and a password, and sometimes additional information like a VPN server address

2) Install VPN Software (if required):

- Any Corp may offer custom VPN client software. If they do, you should download and install this software on your computer or device.

3) Configure VPN Settings (if using built-in clients):

- If Any Corp uses standard VPN protocols (e.g., PPTP, L2TP, IPSec, OpenVPN), you can configure the VPN connection using the built-in VPN clients of your operating system. Here are the general steps for Windows and macOS:
    - Windows:
        - Go to "Settings" > "Network & Internet" > "VPN."
        - Click "Add a VPN connection" and enter the provided VPN server address, your username, and password.
        - You may need to configure additional settings based on your company's VPN requirements.
    - macOS:
        - Go to "System Preferences" > "Network."
        - Click the "+" button to add a new network connection, then choose "VPN."
        - Follow the prompts to configure the VPN settings, including the server address, your username, and password.

4) Mobile Device Configuration (if needed):

- If you need to connect to Any Corp's VPN on a mobile device (iOS or Android), you can usually find VPN settings in the device's network or connection settings. Enter the VPN details provided by your IT department.

5) Manual Configuration (if necessary):

- If you don't have custom VPN software and need to set up the VPN manually, you will require specific information such as:
    - VPN server address or hostname
    - VPN protocol (e.g., PPTP, L2TP, IPSec, OpenVPN)
    - Username and password
    - Any additional settings or certificates required

6) Connect to the VPN:

- Open the VPN client or use the built-in VPN settings, then enter the provided information. Click "Connect" to establish the VPN connection.

7) Authentication:

- You will likely be prompted to enter your username and password to authenticate yourself. If Any Corp uses two-factor authentication (2FA), follow the additional steps as required.

8) Access Corporate Resources:

- Once connected to the VPN, your internet traffic will be routed through Any Corp's network, and you will have access to company resources that are typically available only within the corporate network.

9) Disconnect:

- Remember to disconnect from the VPN when you no longer need it to ensure that your internet traffic returns to its regular route.

10) Q: Can you help me set up a secure password for my accounts?

A:

1) Length:

   - Make your password at least 12 characters long. Longer passwords are generally stronger.

2) Complexity:

   - Use a mix of characters, including uppercase letters, lowercase letters, numbers, and special symbols (e.g., !, @, #, $, %, etc.). The more character types you use, the stronger your password.

3) Avoid Common Words:

   - Avoid using easily guessable words, such as "password," "123456," or common dictionary words. Hackers use dictionary attacks to guess passwords.

4) Avoid Personal Information:

   - Don't use personal information like your name, birthdate, or family members' names. This information is often publicly available on social media.

5) No Sequential or Repeated Characters:

   - Avoid sequences like "123456" or "abcdef," and don't repeat characters like "aaaa."

6) Passphrases:

   - Consider using a passphrase, which is a series of random words or a memorable phrase. For example, "PurpleTiger$DancesUnderMoonlight!"

7) Avoid Easily Guessable Patterns:

   - Don't use patterns like "qwerty" or "asdfgh."

8) Unique Passwords for Each Account:

- Avoid using the same password for multiple accounts. Use a different, unique password for each account you have.

9) Password Managers:

- Consider using a reputable password manager to generate, store, and autofill your passwords. Password managers can help you create and manage complex passwords without having to remember them all.

10) Change Passwords Regularly:

- It's a good practice to change your passwords periodically, especially for important accounts.

Q: What does NashTech Business Process Outsourcing Team does?

A: NashTech has 2000 employees supporting hundreds of clients across multiple different industries segments including retail & e-Commerce, technology, BFSI (banking, financial services & insurance), education, FMCG, manufacturing, professional services, and transportation. We handle more than 20 million data transactions per month in 28 languages with exceptional outcomes. Our delivery centers are based in Vietnam and offer competitive cost advantage when compared to running inhouse operations. We consistently help drive operational costs for our clients down by 30% to 50%, offering flexible teams which can be quickly ramped up and down to match your requirements. We provide leadership expertise in areas of business process outsourcing, process automation solutions and business process re-engineering. Our skilled teams help you undertake the first step of mapping your current processes and perform critical business analysis to determine how you can improve productivity and reduce waste in your process landscape. We have skilled professionals working in the following areas:

Data processing: Including data acquisition, data input, data migration, data preparation for machine learning, data labelling and categorization.

Data quality management: Including verifying, standardizing, and auditing data.

Language services: NashTech can support business process outsourcing in over 28 languages.

Sales and Marketing support: Including customer experience, promotional services and support for Sales and Marketing, including campaign management and Customer Relationship administration.

Digitization: Including content extraction and validation, paper to digital conversion, document management.

Back-office operations: HR & admin support, image processing, financial service, claim administration.

Market research: Including market data collection, consolidation, analysis, and reporting.

Content enrichment: Digital content enrichments, validation and management including but not limited to website, mobile apps, online platform.