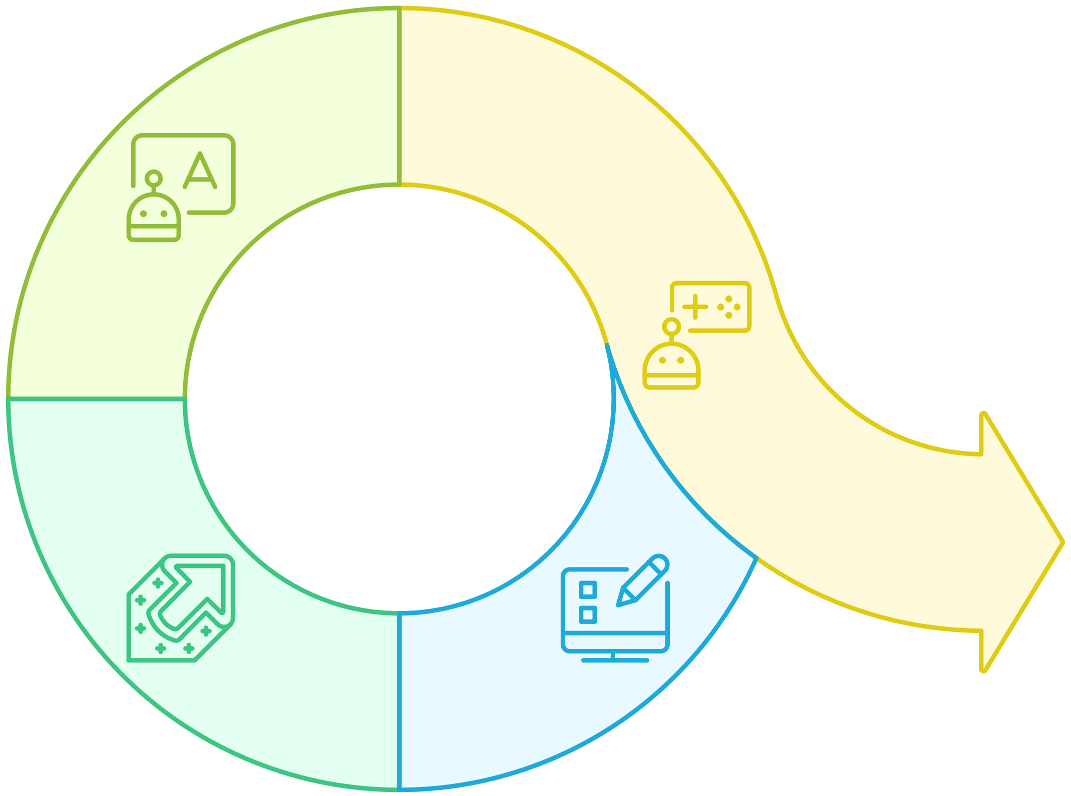
Introduction

What is Prompt Engineering?

Prompt engineering is the art and science of crafting effective inputs (prompts) to guide AI tools like ChatGPT in generating accurate, relevant, and high-quality outputs. By using specific techniques like role-based prompting, few-shot prompting, and chain-of-thought prompting, professionals can automate routine tasks, boost productivity, and streamline workflows.

The Cycle of Prompt Engineering



1

Design Prompts

Create initial prompts for AI interaction

2

Refine Prompts

Improve prompts based on AI responses

3

Enhance AI Performance

Achieve better AI outputs

4

Maximize AI Potential

Utilize AI for diverse applications

Made with Napkin

Choose a Focus Area or Role:

System administrator

Munera Administratoris Systematis

Installation & Configuration

Software et hardware in systematibus computatoriis erigendi.

Sustentatio

Systemata computatoria et retia curandi ut recte operentur.

Securitas

Systemata computatoria et retia contra minas protegendi.

Solutio Problematum

Problematum computatoriorum et reticulorum solvendi.

Auxilium Usoris

Auxilium et sustentationem usoribus praebendi.

Made with Napkin

Common Tasks in That Role: System Administrator

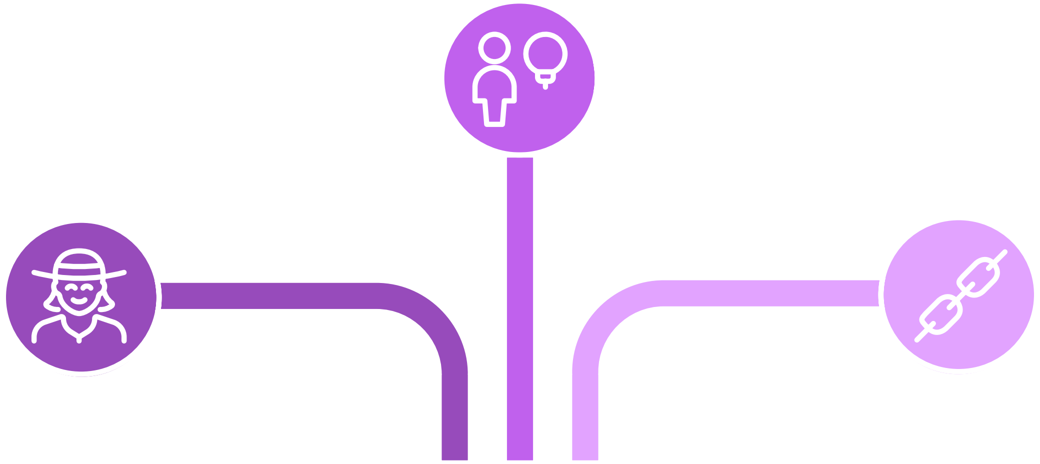
Prompting types:

Role-based Prompting

Few-shot Prompting

Chain-of-thought

Which prompting strategy should be used for AI model interaction?



Few-shot Prompting

Improves accuracy with minimal examples.

Role-based Prompting

Enhances model performance by assigning specific roles.

Chain-of-thought

Enables complex reasoning by breaking down tasks.

Role-based Prompting:

1. Wrting system maintenance reports

Prompt

You are a system administrator. Write a professional weekly maintenance report for the network servers, including tasks performed, issues found, and suggested actions.

📅 Weekly Maintenance ReportPrepared By: System AdministratorWeek Ending: May 14, 2025Department: IT InfrastructureLocation: [Your Organization Name or Data Center Location]

✅ Tasks Performed

Task Description
Server(s) Affected
Status
Performed routine OS patching
All Linux and Windows servers
Completed
Updated antivirus definitions
Mail and File Servers
Completed

Web, DB, Auth Servers

Completed

Backed up critical data to offsite location

DB01, FS02

Successful

Checked RAID health and disk space usage

All storage servers

No issues found

Verified UPS battery status and runtime

Core Network Rack

OK

Applied firmware updates

FW01, SW03

Completed

Tested restore process from backup snapshots

DB01

Successful

Suggested Actions / Recommendations

- Optimize resource usage on APP01: Investigate load balancing options or schedule intensive jobs during off-peak hours.
- Upgrade SSL Certificate on Web02: Apply new certificate before expiry to maintain secure access.
- Network Timeout Mitigation: Evaluate backup window and increase bandwidth allocation for FS01.

for privileged access.

- Conduct Internal Audit: Perform an audit of access logs and firewall rules, especially after blocked login attempts.

Summary & Notes

The overall health of the network infrastructure remains stable. Preventative maintenance tasks were successfully completed. Minor issues were identified and are being addressed accordingly. No critical downtimes occurred during the week.

Approved By:[Your Name]System Administrator[Contact Information]

Few shot prompting

2: Responding to a Server Downtime Incident

prompt

You are a senior system administrator. Below is an example of a message explaining a server downtime incident. Use it as a reference to write a similar message about a recent 2-hour downtime. Example Message: "The email server experienced a 3-hour downtime due to a failed hardware component. The issue was resolved by replacing the faulty part, and normal operations resumed immediately. To prevent future incidents, we will monitor hardware status more frequently and replace aging components proactively." Now, based on this, write a message explaining a 2-hour downtime that occurred due to network congestion, how it was fixed, and steps to prevent it from happening again. 📝 Sample Output: Subject: Server Downtime Incident – May 12, 2025 On May 12, our web server experienced a 2-hour downtime due to network congestion caused by a bottleneck in the routing infrastructure. The issue was quickly resolved by rerouting traffic through an alternative path and resetting the affected switches. Moving forward, we will implement automatic traffic rerouting and monitor network bandwidth more closely to prevent similar incidents in the future.

📢 Incident Report: Server Downtime (Resolved)Date: May 14, 2025Duration: 2 hours (10:15 AM – 12:15 PM)

Team,
This is to inform you about the 2-hour unplanned downtime affecting our primary application server (APP01) earlier today.
🛠️‼️ Cause of Downtime

The root cause was traced to a failed automated update that conflicted with a critical system dependency. Specifically, a security patch applied during the early hours initiated a service restart, but due to an unregistered dependency issue, the application service failed to come back online as expected.

✅ Resolution

- The server was placed in maintenance mode to prevent user disruption.
- Logs were reviewed and the dependency conflict was identified.
- The conflicting patch was rolled back.
- System dependencies were re-verified and the service was restarted manually.
- Full functionality was restored by 12:15 PM.

🔒 Next Steps for Prevention

- A hold has been placed on all automated patching for critical servers pending manual review.
- A pre-patch validation script will be implemented to check service dependencies before updates.
- A monitoring alert has been configured to notify IT immediately if core services fail to restart post-update.
- A post-patch verification checklist will now be followed for all production servers.

We appreciate your patience and understanding. Please reach out if you experience any lingering issues or have questions.

Thanks,[Your Name]System Administrator*internal IT Team*

Chain-of-thought prompt

3: Creating IT Policies

Prompt

“I need a policy on password management for the company. The purpose is to increase security and prevent unauthorized access to sensitive data. The scope should include all employees and contractors who use company systems. The policy should require complex passwords, password changes every 90 days, and multi-factor authentication for remote access. What should the enforcement measures and review process look like?”

Acceptable Use Policy (AUP): Company Wi-Fi and Personal Devices
Document Version: 1.0Effective Date: May 14, 2025Prepared By: IT Department / System AdministratorApproved By: [IT Manager / CIO / HR Department]

1. Purpose

This policy outlines the acceptable use of company-provided Wi-Fi and the responsibilities of employees who connect personal devices (BYOD - Bring Your Own Device) to the company network. Its goal is to protect the integrity, confidentiality, and availability of our IT infrastructure and data.

2. Scope

This policy applies to:

- All employees, contractors, consultants, and temporary staff.
- All devices connecting to the corporate network via company Wi-Fi, including laptops, smartphones, tablets, and IoT devices.

3. Acceptable Use of Company Wi-Fi

Employees may use the company Wi-Fi under the following conditions:

- Business Use Priority: Wi-Fi must primarily support work-related tasks, such as email, communication tools, cloud apps, remote access, and file sharing.
- Limited Personal Use: Occasional personal use is permitted (e.g., checking personal email or browsing news) if it does not interfere with productivity or consume excessive bandwidth.
- Prohibited Activities: The following activities are strictly forbidden:
    - Accessing, downloading, or sharing illegal or offensive content.
    - Streaming high-bandwidth media unrelated to work (e.g., Netflix, YouTube) during business hours.
    - Conducting any form of cryptocurrency mining or unauthorized file sharing (e.g., torrents).
    - Attempting to bypass security protocols, including firewalls or VPN restrictions.

4. Use of Personal Devices (BYOD)

Employees may connect personal devices to the network under the following guidelines:

- Security Requirements:
    - Devices must have up-to-date antivirus software.
    - Operating systems and apps must be updated regularly.
    - Screen lock/passcode must be enabled on all devices.
- Network Access Restrictions:
    - Personal devices will connect to the Guest Wi-Fi or a separate BYOD VLAN with restricted access.
    - Access to sensitive internal systems or confidential data is not permitted from personal devices unless explicitly authorized.
- Data Protection:
    - The company reserves the right to restrict or revoke access if a device is found to pose a security risk.
    - Employees must report lost or stolen personal devices that were connected to the company network.

5. Monitoring and Enforcement

- All network traffic may be monitored to ensure compliance with this policy.
- Violations may result in:
    - Temporary or permanent suspension of network access.
    - Disciplinary action up to and including termination.
    - Legal action in the case of severe violations.

6. Employee Acknowledgment
All employees must acknowledge that they have read, understood, and agreed to abide by this policy. An annual review and re-signature may be required.
For Questions or Reporting Issues:Contact the IT Help Desk at [helpdesk@company.com] or call [extension].
[Your Name]System Administrator[Your Company Name][Contact Information]

Role-based Prompting

4: Providing Troubleshooting Support

Prompt

You are a system administrator assisting a junior colleague. Provide a step-by-step troubleshooting guide for resolving "No Internet Access" on a company workstation.

Objective: Restore internet connectivity on a workstation while identifying the root cause.

✅ Step 1: Initial Checks

1. Confirm the symptom:
    - Check if the workstation shows “No Internet” in the taskbar.
    - Attempt to open multiple websites (e.g., www.google.com, www.microsoft.com).
    - Check if any internal resources (e.g., shared drives, intranet) are accessible.
2. Check physical connections:
    - For wired: Ensure Ethernet cable is securely plugged into both the workstation and the switch or wall port.
    - For Wi-Fi: Confirm the device is connected to the correct SSID.

🔍 Step 2: Verify IP Configuration

1. Open Command Prompt and run:

bash

CopyEdit

```
ipconfig /all
```

1. Check for:
    - Valid IP address (e.g., not 169.254.x.x)
    - Default gateway present
    - DNS server addresses listed
2. Release and renew the IP address:

bash

CopyEdit

```
ipconfig /release
ipconfig /renew
```

1. Ping the loopback address to ensure TCP/IP stack is working:

nginx

CopyEdit

```
ping 127.0.0.1
```

2. Ping the default gateway:

css

CopyEdit

```
ping [gateway IP address]
```

3. Ping a public IP (e.g., Google DNS):

nginx

CopyEdit

```
ping 8.8.8.8
```

4. Ping a domain name:

nginx

CopyEdit

```
ping google.com
```

4. If this fails but step 3 succeeds, it’s likely a DNS issue.

🔧 Step 4: Check DNS Settings

1. Check DNS Server settings in adapter properties:
    - Go to *Network and Sharing Center > Change adapter settings > Right-click > Properties > IPv4 > Properties*.
    - Use company DNS or fallback to 8.8.8.8 (Google) for testing.
2. Flush DNS cache:

bash

CopyEdit

🖥️‼️ Step 5: Restart Network Services

1. In Command Prompt (run as Admin), restart network stack:

perl

CopyEdit

```
netsh winsock reset
netsh int ip reset
```

2. Reboot the machine.

🧰 Step 6: Check Device Manager and Firewall

1. Open Device Manager:
    - Expand “Network Adapters”.
    - Ensure the adapter is enabled and has no warning icons.
    - Optionally, uninstall and reinstall the driver.
2. Check Windows Firewall or Antivirus:
    - Temporarily disable to rule out blockage (enable it afterward).

🌐 Step 7: Try Alternate Network

1. Connect the workstation to:
    - Another Ethernet port or Wi-Fi network.
    - A mobile hotspot (to rule out company network issue).
2. If internet works elsewhere, escalate to network team for potential switch/router/VLAN misconfigurations.

📋 Step 8: Escalate if Unresolved

If none of the above resolve the issue:

- Log details of all steps tried.
- Note MAC address, hostname, IP config, and time of issue.
- Escalate to senior admin or network engineer for deeper diagnostics.

Role-based Prompting

Task 5: Drafting a User Onboarding Email

Prompt

Imagine you’re a system administrator. Write a welcome email for new employees explaining how to set up their workstation, access the intranet, and contact IT support.

Subject: 👋 Welcome to [Company Name] – Workstation Setup & IT Support Info
Hi [New Employee’s First Name],
Welcome to [Company Name]! We’re excited to have you on board.
To help you get started smoothly, please find below the essential steps to set up your workstation, access company resources, and reach out to IT support if you need assistance.
💻‼ Workstation Setup

1. Log in to your workstation
    - Username: firstname.lastname
    - Temporary Password: Welcome@123 (You’ll be prompted to change it on first login.)
2. Connect to the Company Wi-Fi
    - SSID: Company-WiFi
    - Password: Provided on your desk card

    - Alternatively, use the Ethernet cable for a direct connection (recommended for desktops).
3. Set Up Email & Calendar
    - Open Outlook or visit webmail.company.com
    - Sign in with your company credentials.
4. Install Required Applications
    - Use the Company Software Portal (shortcut on your desktop) to install apps like Microsoft Teams, VPN, and company-specific tools.

🌐 Intranet Access

- Go to: intranet.company.com
- Here you'll find:
    - Company news & announcements
    - HR policies and forms
    - Department contacts
    - Resource links and team directories

🛠‼ IT Support

If you run into any technical issues or need help:

📧 Email: itsupport@company.com 📞 Call: Ext. 1010 💬 Chat: Via Teams > IT Help Desk channel 📍 Walk-in: IT Office – 2nd Floor, Room 204 (Hours: 9 AM – 5 PM)

Please don't hesitate to reach out if you have questions—we're here to help you get settled in.

Once again, welcome aboard! We're glad you're here.

Best regards,[Your Name]System Administrator[Company Name][Contact Info]

Task 4: Test and Improve Prompts

Before

Write an email about password changes.

Subject: 🔐 Mandatory Password Change Notification

Dear Team,

As part of our ongoing efforts to enhance information security and comply with internal IT policies, all employees are required to change their account passwords by [insert deadline, e.g., Friday, May 17, 2025].

🔁 How to Change Your Password:

1. Press Ctrl + Alt + Delete on your keyboard.
2. Click “Change a password”.
3. Enter your current password, then your new password.
4. Confirm and submit.

- Minimum 8 characters
- Must include uppercase, lowercase, number, and special character
- Cannot be the same as the last 5 passwords
- Avoid using personal information (e.g., names, birthdates)

🔒 Best Practices:

- Do not share your password with anyone.
- Use a unique password for your company account (not reused from other services).
- Consider using a secure password manager to store your credentials.

If you encounter any issues or need assistance, please contact the IT Help Desk:

✉ itsupport@company.com 📞 Ext. 1010 💬 Teams > IT Help Desk

Thank you for your cooperation in keeping our systems secure.

Best regards,[Your Name]System Administrator[Company Name]

After

As a system admin, draft an email to staff about a new password policy. First explain why, then list rules, and state the effective date.

Subject: 🔐 New Password Policy – Effective [Insert Date]

Dear Team,

To enhance the security of our systems and protect company and client data, we are implementing a new password policy aligned with industry best practices and compliance standards.

Cyber threats continue to evolve, and strong password hygiene is one of our first lines of defense. This updated policy is designed to reduce risk and safeguard our digital environment.

🔑 New Password Policy Rules:

Effective [Insert Date, e.g., Monday, May 20, 2025], all staff must follow these password rules:

- Minimum Length: 12 characters
- Complexity: Must include at least one uppercase letter, one lowercase letter, one number, and one special character
- Expiration: Passwords must be changed every 90 days
- Reuse Restrictions: Cannot reuse any of your last 5 passwords
- Lockout Policy: After 5 failed login attempts, the account will be locked for 15 minutes
- MFA Enforcement: Multi-Factor Authentication is required for all remote and administrative access

💬 What You Need to Do:

You will be prompted to update your password at your next login after the policy takes effect. We recommend thinking ahead and preparing a secure passphrase or using a password manager.
For questions or help resetting your password, please contact:
✉ itsupport@company.com 📞 Ext. 1010 💬 Teams > IT Help Desk

Thank you for your attention and commitment to keeping our systems secure.
Best regards,[Your Name]System Administrator[Company Name]

Before

Write an FAQ about account lockouts.

Account Lockout FAQ
1. What is an account lockout?
An account lockout occurs when your user account is temporarily disabled after multiple failed login attempts. This is a security measure to protect your account from unauthorized access.
2. What causes an account to lock out?
Common causes include:

- Entering the wrong password repeatedly (typically 5 times or more)
- A saved password in a background app (e.g., Outlook, mobile device) that is no longer valid
- Syncing issues with mapped drives or scheduled tasks using old credentials
- Attempting to log in on multiple devices with incorrect credentials

3. How long does a lockout last?

By default, accounts are locked for 15 minutes. After this period, you may try logging in again. If your account does not unlock, please contact IT support.

4. How can I unlock my account faster?

Contact the IT Help Desk to manually unlock your account:

- 📧 Email: itsupport@company.com
- 📞 Phone: Ext. 1010
- 💬 Teams: IT Help Desk channel

5. How can I avoid account lockouts?

- Make sure your password is updated on all devices (desktop, phone, tablet, etc.).
- Update credentials in Outlook, VPN, mobile mail apps, and any other saved login services after a password change.
- Avoid using incorrect or outdated passwords repeatedly.
- Use a password manager to ensure accuracy.

6. I keep getting locked out even after resetting my password. Why?

This usually means one of your devices or apps is still using an old password. Common culprits include:

- Email accounts on your smartphone or tablet
- VPN clients

- Background services or scheduled tasksIT can help you identify and clear these sources if needed.

7. Will I be notified when I’m locked out?
You may receive a notification on your login screen, or a message such as:“Your account has been locked. Please contact your administrator.”If you suspect a lockout but don't see this message, contact IT to confirm.

After (Improved with Role-Based Prompting):

You are a system administrator responsible for IT support. Create a clear FAQ for employees explaining what to do if their account gets locked after multiple failed login attempts. Include step-by-step guidance and support contact info.
Account Locked? Here’s What to Do
Why did my account get locked?
Your account is automatically locked after 5 consecutive failed login attempts. This security feature protects against unauthorized access.
What should I do if my account is locked?
☑ Step-by-Step Instructions:

1. Wait 15 minutes
    - Most account locks reset automatically after a 15-minute period.
    - After waiting, try logging in again with the correct credentials.
2. Double-check your credentials
    - Ensure you’re using the correct username and the most recent password.

    - If you recently changed your password, remember to update it on all devices (e.g., phone, tablet, VPN client).
3. Still locked out? Contact IT SupportIf waiting doesn't resolve the issue or you're unsure about your password, reach out to IT for assistance.

📞 How to Contact IT Support

IT Help Desk Contact Info:

- 📧 Email: itsupport@company.com
- 📞 Phone: Ext. 1010
- 💬 Teams Chat: IT Help Desk
- 🕘 Hours: Monday–Friday, 9:00 AM – 5:00 PM

When contacting us, please include:

- Your full name
- Your username
- A short description of the issue (e.g., "Account locked after password change")

🛡️‼️ Tips to Prevent Future Lockouts

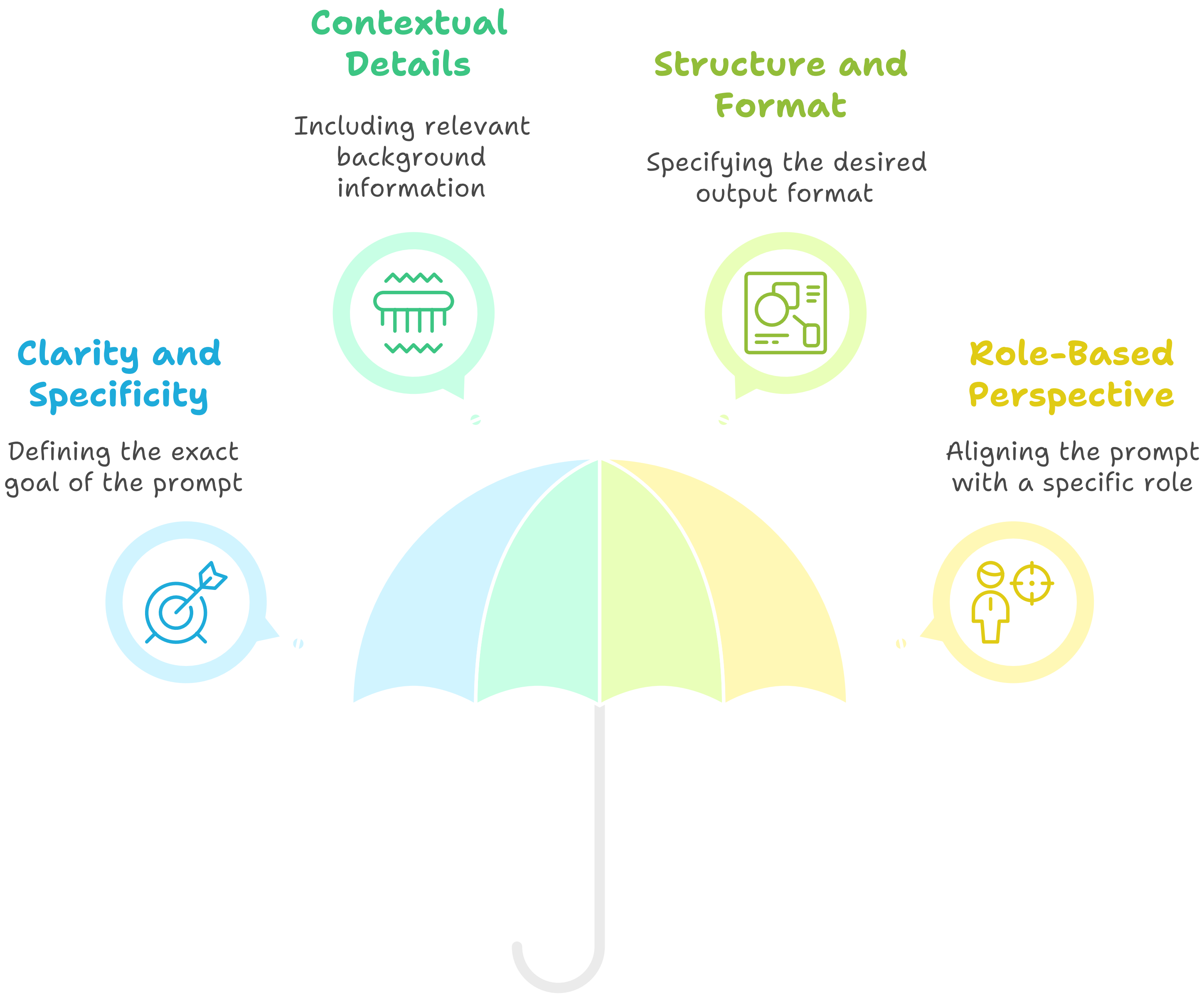
- Update your password on all devices immediately after changing it.
- Avoid using old saved credentials in apps like Outlook, VPN, or mobile mail.
- Use a password manager to reduce typos and re-entry errors.

If you have any questions or concerns, don't hesitate to reach out. We're here to help!
– IT Department[Company Name]

☑️ Tips for Writing Effective Prompts (System Admin Role)

1. Be Clear and Specific
    - Define the exact goal: Are you writing a policy, troubleshooting, or drafting a communication?
    - Example: *“Write a step-by-step guide for resetting a user’s AD password remotely using PowerShell.”*
2. Provide Context
    - Include relevant details: system environment, audience (users vs. IT staff), timeframe, or specific tools (e.g., Windows Server 2022, Office 365, Fortinet).
    - Example: *“Create a backup policy for Windows-based servers in a mid-sized organization with 50 virtual machines.”*
3. Request Structure or Format
    - Ask for content in bullet points, numbered steps, or formal document format (e.g., policy, SOP, email, FAQ).
    - Example: *“Write an internal memo in email format explaining the new MFA policy.”*
4. Use Role-Based Perspective
    - Start with: *“You are a senior system administrator…”* or *“Act as an IT support specialist…”* This ensures responses are relevant to your role.

Enhancing Prompt Effectiveness



Contextual Details

Including relevant background information

Structure and Format

Specifying the desired output format

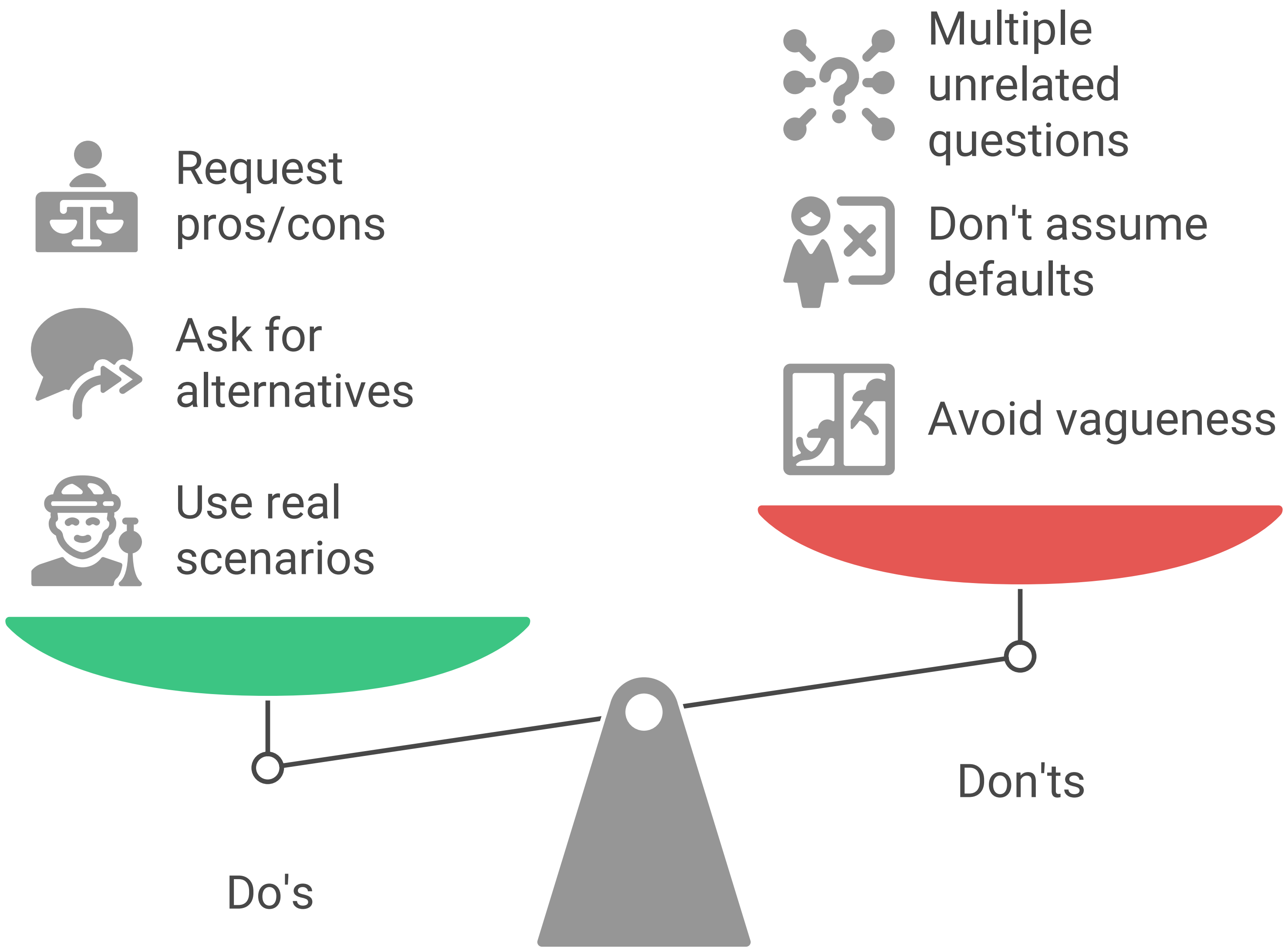
Clarity and Specificity

Defining the exact goal of the prompt

Role-Based Perspective

Aligning the prompt with a specific role

Made with Napkin



- Request pros/cons
- Ask for alternatives
- Use real scenarios

Do's

- Multiple unrelated questions
- Don't assume defaults
- Avoid vagueness

Don'ts

Maximize clarity and effectiveness in communication.

Made with Napkin