LIST OF DOCUMENTS

Sl.No	Description
1	IT Policy
2	IT facilities Update details
3	Wi-Fi details
4	Software details
5	Bandwidth for internet connection
6	Service provider agreement

1.NEED FOR IT POLICY

- The IT policy of the institution exists to maintain, secure, and ensure the legal and appropriate use of the information technology infrastructure established on campus.
- This policy defines institutional strategies and responsibilities for protecting the confidentiality, integrity, and availability of information assets that are accessed, created, or managed.
- The IT policy is documented to ensure fair and transparent use of various IT resources across the campus for academic purposes. It applies to students, faculty, staff, management, visiting guests, and research fellowship members.

Dhanraj Baid Jain College now has network connections to every computer system, covering all buildings across the campus and the hostel.

The System Administrator is responsible for managing the institute's internet services. This includes overseeing firewall security, DHCP, DNS, email, web services, and overall network management for the college.

Previously, the college utilized a 200 Mbps internet leased line from BSNL, which has now been upgraded to a 150 Mbps connection provided by Tikona. With extensive internet usage, the network performance has improved in three key ways.

- Compared to the speed of the Local Area Network (LAN), internet traffic over the Wide Area Network (WAN) can create a bottleneck.
- When users have unrestricted internet access, non-essential downloads can congest the network, leading to poor service quality and impacting critical users and applications.
- In a networked environment, viruses entering the LAN through the intranet or internet can quickly spread to all connected computers, exploiting operating system vulnerabilities.

Too many concurrent users on the high-speed LAN accessing internet resources through limited bandwidth can strain the available internet capacity. Every download adds to this traffic, increasing costs and ultimately degrading the quality of service and user experience. Reducing internet traffic is essential to maintain performance.

Computer viruses attach themselves to files, spreading rapidly when these files are shared. Some viruses can damage files or even reformat the hard drive, causing significant losses. Others simply replicate themselves, consuming network resources and slowing down performance. Moreover, substantial employee time is lost when workstations must be scanned and cleaned due to virus infections from emails, unsafe downloads, file sharing, and web sharing. Once they enter the network, viruses replicate quickly, causing severe damage, slowing down, or even halting network operations.

Containing a virus once it spreads through the network is challenging, consuming both time and resources to restore network safety. Preventive measures are crucial. To secure the network, the System Administrator has implemented firewalls, access controls, and virus-checking and content-filtering software at the gateway. However, without clearly defined IT policies, it can be challenging to convince users of the necessity of these steps. Users may feel that these restrictions are unwarranted, unjustified, and infringe upon their freedom.

As IT users know, educational institutions worldwide have implemented IT policies to guide technology use. Without strong management policies, IT security measures may be ineffective and not necessarily aligned with management objectives. Furthermore, due to the dynamic nature of information technology, information security policies must also be adaptable. Regular review and updates are essential to accommodate changing technologies, evolving user needs, and updated operating procedures.

IT policies can be classified into the following categories:

- ✓ IT Hardware Installation Policy
- ✓ Software Installation and Licensing Policy
- ✓ Network (Intranet/Internet) User Policy
- ✓ Email Account User Policy
- ✓ Website Hosting Policy
- ✓ Additionally, these policies will apply at two levels:
- ✓ End User Groups: This includes faculty members, students, senior administrators, officers, and other staff members.

Network Administration

The institute's IT policy applies to technology managed either centrally by the institute or by individual departments. This includes information services provided by the institute administration, individual departments, members of the institute community, or authorized visitors, whether resident or non-resident, who connect their own devices to the institute network.

This IT policy also extends to resources managed by central administrative departments, such as the library, computer laboratories, offices, hostels, guest houses, and residences where the network facility is provided by the institute.

Furthermore, all faculty, students, staff, departments, authorized visitors, and visiting faculty who are granted access to the institute’s IT infrastructure must adhere to these guidelines. Violations of the institute's IT policy by any member of the institute may result in disciplinary action. If illegal activities are involved, law enforcement agencies may be involved.

The purpose of the IT policy is to establish direction and provide information on acceptable actions, as well as to define prohibited actions and policy violations.

Applies To

Stakeholders, both on and off campus, include:

Students: Undergraduate and Postgraduate

Employees

Faculty

Administrative Staff: Technical and Non-Technical

Higher Authorities and Officers

Guests

Resources

Network Devices (Wired/Wireless):

Internet Access

Official Websites and Web Applications

Official Email Services

Data Storage

Mobile/Desktop/Server Computing Facilities

Document Facilities: Printers and Scanners

Multimedia Content

2. IT Hardware Installation Policy

The institute's network user community must follow certain precautions when installing computers or peripherals to minimize service interruptions caused by hardware failures.

a) Primary User

The primary user is defined as the individual who primarily uses the computer installed in their workspace. If a computer is shared by multiple users with no designated primary user, the department head should assign someone responsible for ensuring compliance with this policy.

b) End-User Computer Systems

In addition to client PCs, the institute considers servers not directly managed by the Computer Centre as end-user computers. If no primary user is identified, the department must assume end-user responsibilities. Any servers providing services over the intranet or internet, registered with the Computer Centre, are also considered "end-user" computers under this policy.

c) Warranty & Annual Maintenance Contract

Computers purchased by any department or unit should preferably come with a three-year on-site comprehensive warranty. After the warranty expires, maintenance will be provided by the System Administrator or external service engineers on an as-needed basis. This maintenance includes OS reinstallation and addressing virus-related issues.

d) Power Connection to Computers and Peripherals

All computers and peripherals must be connected to a UPS. The UPS power supply should remain on at all times to ensure continuous battery recharging. UPS systems must also be connected to properly earthed electrical points with secure wiring.

e) Network Cable Connection

When connecting a computer to the network, ensure that network cables are kept away from electrical or electronic equipment to prevent interference. Additionally, the power supply for computers and peripherals should not be shared with other electrical or electronic equipment.

f) File and Print Sharing Facilities

File and print sharing over the network should only be enabled when absolutely necessary. Shared files should be password-protected and set to read-only access.

g) Maintenance of Computer Systems Provided by the Institute

The System Administrator will handle maintenance issues for institute-purchased computers distributed centrally, based on any reported problems.

h) Noncompliance

Noncompliance with this computer hardware installation policy by faculty, staff, or students at Dhanraj Baid Jain College can create network-related risks, potentially resulting in data loss, inoperable computers, and reduced productivity. Non-compliant devices can negatively impact other individuals, groups, departments, or the entire institute. It is crucial to address any compliance issues promptly.

Computer Centre Interface

If the System Administrator identifies a non-compliant computer affecting the network, they will notify the responsible individual via email or phone, requesting compliance. The notified user must ensure their computer achieves compliance promptly, with guidance provided by the System Administrator as needed.

3. Software Installation and Licensing Policy

Departments or units purchasing computers must ensure that all systems are equipped with licensed software, including the operating system, antivirus software, and any necessary application software. In compliance with anti-piracy laws, the institute's IT policy prohibits the installation of pirated or unauthorized software on institute-owned computers and those connected to the campus network. In cases of violation, the institute will hold the respective department or individual accountable for any pirated software installed in their department or personal workspace.

a) Operating System and Its Updating

Users must ensure their computer systems have the latest operating system updates, including service packs and patches, downloaded from the internet. This is particularly crucial for all MS Windows-based computers, as Microsoft periodically releases updates to fix vulnerabilities.

b) Antivirus Software and Its Updating

All computer systems in the institute must have active antivirus software installed. The primary user is responsible for ensuring compliance with this virus protection policy, including maintaining current antivirus software. Users should verify that their antivirus software is functioning correctly; outdated or unrenewed antivirus software is ineffective. If users find these responsibilities beyond their technical abilities, they should seek assistance from the System Administrator.

c) Backups of Data

Users should conduct regular backups of their essential data, as virus infections can destroy files on individual computers. Without proper backups, recovering lost files may be impossible. Ideally, during OS installation, the hard disk should be partitioned into multiple volumes (e.g., C, D). The OS and software should reside on the C drive, while user data files should be stored on other drives (e.g., D, E). This practice can help mitigate data loss in case of virus issues, though it is not foolproof. Additionally, users should store valuable data on CDs, DVDs, or external storage devices such as pen drives or external hard drives.

d) Noncompliance

Faculty, staff, and students at Dhanraj Baid Jain College who do not adhere to this computer security policy expose themselves and others to risks of virus infections, potentially leading to damaged or lost files and inoperable computers, resulting in productivity loss. There is also a risk of spreading infections and unauthorized access to confidential data. A single non-compliant computer can have significant adverse effects on groups, departments, or even the entire institute. It is essential to ensure that all computers comply as soon as non-compliance is identified.

e) System Administrator Interface

If the System Administrator identifies a non-compliant computer, they will notify the responsible individual via email or phone, requesting compliance. The notified user must ensure their computer achieves compliance promptly, following up as necessary. The System Administrator will provide guidance to assist the individual in achieving compliance.

4. Network (Intranet & Internet) Use Policy

The network connectivity provided through an authenticated network access connection or Wi-Fi is regulated by the Institute IT Policy. The System Administrator is responsible for the ongoing maintenance and support of the network, excluding local applications. Any issues within the institute’s network should be reported to the computer center.

All computers (PCs/servers) connecting to the institute network must have an IP address assigned by the computer center. Departments should adhere to a systematic approach regarding the allocation of IP addresses, with specific ranges designated for each building or WLAN. Therefore, any computer connected to the network in a particular building will be assigned an IP address only from that location. Each computer will have a binding association with its IP address, ensuring that no unauthorized users can access that IP from different locations. Users must obtain IP address allocations from the System Administrator for their respective departments.

An IP address allocated to a specific computer system should not be used for any other computer belonging to the same individual when connected to the same port. IP addresses are assigned to computers, not to the ports.

a) DHCP and Proxy Configuration by Individual Departments/Cells/Users

Using any computer at the end-user location as a Dynamic Host Configuration Protocol (DHCP) server to connect multiple computers through an individual switch or hub and distribute IP addresses (public or private) is strictly prohibited, as it violates the institute's IP address allocation policy. Similarly, configuring proxy servers is not allowed, as it may interfere with services managed by the computer center. Non-compliance with the IP address allocation policy will result in the disconnection of the port from which the non-compliant computer is connected. The connection will only be restored after receiving a written assurance of compliance from the concerned department or user.

b) Running Network Services on the Servers

The System Administrator does not assume responsibility for the content of machines connected to the network, regardless of whether those machines are institute-owned or personal property. The System Administrator may disconnect client machines found to have potentially damaging software. A client machine may also be disconnected if its activities adversely affect network performance. The institute’s network and network resources are not to be used for personal or commercial purposes. Network traffic will be monitored for security and performance reasons. Any violation of this agreement may result in the termination of the connection.

c) Dial-up/Broadband Connection

Computer systems that are part of the institute's campus-wide network, whether institute-owned or personal property, must not be used for dial-up or broadband connections, as this violates institute security protocols by bypassing firewalls and other network monitoring systems. Non-compliance with this policy may result in the withdrawal of the IP address assigned to that computer system.

d) Wireless Local Area Networks

This policy applies to all departmental and hostel wireless local area networks. In addition to the requirements outlined in this policy, departments or hostels must register their access points with the System Administrator, including relevant contact information.

5. Email Account User Policy

To enhance the efficient distribution of critical information to faculty, staff, students, and administrators, it is strongly recommended to utilize the institute's email services for formal communications related to academic and official purposes. Using email for formal communications will facilitate the delivery of messages and documents to the campus community, specific user groups, and individuals. Official communications include administrative content such as human resources information, policy updates, general institute messages, and official announcements.

To ensure receipt of these communications, it is essential to keep your email address active by using it regularly. Staff and faculty can access the email facility by logging in with their username and password. For obtaining an institute email account, users should contact the System Administrator and apply using the prescribed form to receive their account details and default password.

By using the email facility, users agree to adhere to the following policies:

- The email facility should be used primarily for academic and official purposes, with limited personal use allowed.
- Using the facility for illegal or commercial purposes is a direct violation of the institute's IT policy and may result in withdrawal of access. Illegal activities include,

but are not limited to, unlicensed software copying and distribution, sending unsolicited bulk emails, and generating threatening, harassing, abusive, or fraudulent messages or images.

- Users should not open any email or attachment from unknown or suspicious sources. Even emails from known sources should be approached with caution; if an attachment appears dubious, users must confirm its authenticity with the sender before opening it. This is crucial for protecting the user's computer from potential viruses that could damage valuable information.
- Users must not share their email accounts with others, as the individual account holder is personally accountable for any misuse of that email account.
- When using shared computers, users must promptly log out of any email account left open by another user without peeking at its contents.
- Impersonating another user's email account is considered a serious offense under the institute's IT security policy.
- Ultimately, it is the responsibility of each individual to keep their email account compliant with the institute's email usage policy.

The policies outlined above also apply to email services provided by external sources such as www.hotmail.com and www.yahoo.com, as long as they are used for official purposes on the institute's campus, even when accessed from outside the campus.

6. Website Hosting Policy

a) Official Pages

Departments, cells, and central facilities are permitted to have pages on the official Dhanraj Baid Jain College website. Currently, the System Administrator is responsible for maintaining the official website at www.dbjaincollege.org.

b) Personal Pages

Recognizing that individual faculty members may have specific needs for their personal pages, faculty can request to link their pages to the official institute website. To do this, they must submit a written request or email to the System Administrator, providing the URL of the

page they wish to add. However, any illegal or improper usage will result in the termination of the hyperlink.

The content of personal pages must adhere to the following guidelines:

- Must not violate any applicable export laws and regulations.
- Must not infringe on copyright or trademark rights.
- Must not be used for political lobbying.
- Must not violate any local, state, or central government laws.

Additionally, personal pages are not permitted to host content for other individuals or groups.

7. Institute Database Use Policy

This policy pertains to the databases maintained by Dhanraj Baid Jain College. Data is a vital and essential resource for providing valuable information, and its use must be safeguarded, even if the data is not classified as confidential. The college has established its own policies regarding the creation of databases, access to information, and a more general policy on data access. Together, these policies outline the institute's approach to accessing and utilizing this resource.

Database Ownership

Dhanraj Baid Jain College is the owner of all institutional data generated within the institute.

Data Administrators

Data administration responsibilities may be delegated to designated officers within each department. The following Management Information Systems are included in these responsibilities:

- Employee Information Management System
- Student Information Management System
- Financial Information Management System
- Library Information Management System
- Document Management & Information System

General Policy Guidelines

The following guidelines are applicable to data users in departments, cells, and administrative offices:

1. The institute's data policies prohibit the distribution of data that identifies individuals outside the institute.
2. Data from the institute's databases, including data collected by departments or individual faculty and staff, is for internal use only.
3. An individual's role and responsibilities determine the data resources necessary for fulfilling official duties. Access to information and data is granted based on these responsibilities.
4. Personal information that identifies an individual must not be distributed in any form to external persons or agencies, including government entities. All such requests should be directed to the appropriate office for response.
5. Requests for information from courts, attorneys, or other legal entities must be handled by the office; departments should not respond directly to such inquiries. All requests from law enforcement agencies must also be forwarded to the office for appropriate action.
6. Tampering with the database by departments or individual users is considered a violation of IT policy. Tampering includes, but is not limited to:

    - Modifying or deleting data items or software components through unauthorized access methods.
    - Deliberately modifying or deleting data items or software components with malicious intent, even by authorized personnel.
    - Causing a database, hardware, or system software crash that intentionally destroys part or all of the database.
    - Attempting to breach the security of the database.

8. Hostels Wi-Fi Use Policy

The wireless infrastructure in the hostels is designed to enhance internet accessibility for academic purposes and to facilitate access to licensed online resources, such as online journals, for students and faculty members.

Signal availability and strength may vary across different locations within the hostel. It is not guaranteed that every area on each floor of every block will have uniform signal coverage.

Access to the wireless internet is considered an additional service, and students or residents in the hostels cannot demand this service. The availability of wireless connectivity is at the discretion of the institute, which reserves the right to suspend or interrupt the service at any time for technical reasons.

The access points provided in the hostels are the property of the institution. Any damage or loss of this equipment will be regarded as a serious violation of the Dhanraj Baid Jain College (DBJC) code of conduct, and disciplinary action will be taken against any student found responsible for such loss or damage. In the event of loss or damage to the wireless infrastructure, an assessment will be conducted, and the cost of repairs will be recovered from all students residing on the affected floor, building, or hostel.

9. Roles and Responsibilities of the System Administrator

a) Campus Network Backbone Operations

1. The Computer Center is responsible for the administration, maintenance, and control of the campus network backbone and its active components.
2. The System Administrator operates the campus network backbone to ensure that service levels are maintained for the Institute's departments and hostels connected to the network, adhering to operational best practices.

b) Maintenance of Computer Hardware & Peripherals

The System Administrator provides Net Access IDs and email accounts to individual users, enabling them to utilize the campus-wide network and email facilities offered by the institute, upon receiving requests through the prescribed proforma.

Disconnect Authorization

The System Administrator has the authority to disconnect any department, cell, or hostel from the campus network backbone if their traffic violates the practices outlined in this policy or any related network policies. If the normal flow of traffic is significantly disrupted by a department, cell, or hostel, the System Administrator will work to resolve the issue with

minimal impact on other network members. If a department or division is disconnected, the System Administrator will specify the conditions that must be fulfilled for reconnection.

10. Responsibilities of the Department

a) User Account

Any center, department, cell, or entity may connect to the institute network using a legitimate user account for verification of affiliation with the institute. The System Administrator will provide user accounts upon completion of the prescribed application form submitted to them.

Once a user account is allocated for accessing the institute's computer systems, network, email, and web services, the account holder is personally responsible and accountable to the institute for all actions performed using that account. Therefore, users are advised to take reasonable precautions, such as:

- Using complex passwords
- Not sharing passwords with others
- Avoiding writing down passwords in accessible places
- Changing passwords frequently
- Maintaining separate passwords for Net Access IDs and email accounts

These measures help prevent unauthorized use of the institute's resources. Users are also responsible for familiarizing themselves with the institute's IT policy and adhering to the guidelines for the proper use of technology and information resources.

b) Supply of Information by Departments or Cells for Publishing/Updating the Website

All departments or cells must periodically provide updated information about their activities, at least once a month or sooner if necessary. This information can be submitted in hardcopy or softcopy to the System Administrator. This policy also applies to advertisements, tender notifications published in newspapers, and events organized by departments or cells.

Links to any web pages created for specific purposes or events can be established by the System Administrator upon receiving written requests. If these web pages are to be directly added to the official institute website, the respective department or individual must provide the

necessary content (and images, if applicable) in a format compatible with the existing web design. Such requests, along with a soft copy of the content, should be submitted to the System Administrator well in advance.

c) Security

By connecting to the network backbone, departments agree to comply with the network usage policy outlined in the institute's IT security policy. Any network security incidents will be resolved in coordination with a designated point of contact (POC) in the originating department. If a POC is unavailable, the offending computer will be disconnected from the network until compliance is achieved.

d) Preservation of Network Equipment and Accessories

Routers, switches, fiber optic cabling, UTP cabling, connecting inlets to the network, racks, UPS, and their batteries installed at various locations are the property of the institute and are maintained by the System Administrator and the respective department. Tampering with these items by a department or individual user constitutes a violation of IT policy.

e) Additions to the Existing Network

In addition to the above responsibilities, the System Administrator recommends implementing a regular backup strategy. It is important to note that despite all preventive measures, there remains a risk of virus infections or hacker compromises. Regularly backing up data (daily and/or weekly) can significantly mitigate the damage caused by the loss of a machine.

11. Responsibilities of the Administrative Department

The Administrator shall perform duties under the direction of the respective head, encompassing the following responsibilities:

I. **System Requirements and Procurement**: Manage system requirements and related activities, including obtaining quotations for the procurement of hardware and software.

II. **Server Administration**: Administer and configure servers, ensuring optimal system performance through regular tuning.

III. **Website Development and Maintenance**: Oversee the development and maintenance of the institute's websites, ensuring they are up-to-date.

IV. **Software Installation and Maintenance**: Install and maintain software for campus systems, including operating system updates, patches, and configuration changes.

V. **Hardware and Software Configuration**: Install and configure new hardware and software as required.

VI. **Network Administration**: Administer campus-wide LAN and internet services, ensuring network infrastructure is operational.

VII. **Infrastructure Management**: Ensure that the network infrastructure is consistently up and running.

VIII. **Training Programs**: Facilitate the conduct of periodic computer awareness and literacy courses/training programs for students and staff.

IX. **ICT and MIS Implementation**: Identify and assist in the implementation of ICT and Management Information System (MIS) requirements for the institute.

X. **System Analysis**: Analyze system logs to identify potential issues with computer systems.

XI. **Technology Integration**: Introduce and integrate new technologies into the existing data center environment.

XII. **Data Backup**: Perform regular backups of data and files to safeguard information.

XIII. **System Audits**: Conduct routine audits of systems and software to ensure compliance and performance.

XIV. **User Account Management**: Manage user accounts by adding, removing, or updating account information, including resetting passwords as needed.

XV. **Technical Support**: Respond to technical queries and provide assistance to users.

XVI. **Security Responsibility**: Maintain the security of systems and networks, ensuring compliance with established policies.

XVII. **Additional Duties**: Undertake any other tasks assigned from time to time as needed by the head.

12. Video Surveillance Policy

The video surveillance system consists of fixed-position cameras, monitors, digital video recorders, storage, and public information signs. Cameras will be strategically placed, primarily at the entrance and exit points of buildings and sites. All cameras will be visible, and none will focus on the front or rear areas of private accommodations. Signs will be prominently displayed at key locations, including entrance and exit points, to inform staff, students, visitors, and the public about the presence of CCTV cameras.

While every effort has been made to ensure the system's effectiveness, it is not possible to guarantee that every incident within the coverage area will be detected.

Purpose of the System

The system has been installed by the institute primarily to reduce the threat of crime, protect institute premises, and ensure the safety of all staff, students, and visitors, while respecting individual privacy. The objectives of monitoring the system include:

- Deterring individuals with criminal intent
- Assisting in the prevention and detection of crime

- Facilitating the identification, apprehension, and prosecution of offenders related to crimes and public order violations
- Supporting the identification of activities or events that may warrant disciplinary action against staff or providing evidence to managers in cases of disciplinary or other actions against staff or students

It is recognized that individuals may have concerns or complaints regarding the operation of the system. Any complaints should be directed to the Computer Centre. CCTV footage may be provided by the institute upon receiving requests from individuals using the prescribed format.

Campus Network Service Use Agreement

Before applying for a user account or email account, please read the following important policies:

By signing the application for a Net Access ID (user account) or email account, you agree to comply with the IT policies and guidelines of DB Jain. Failure to adhere to these policies may result in the termination of your account or IP address. This is a summary of key IT policies; users can access a detailed document from the institute's website or various internet servers. A Net Access ID consists of a username and password, allowing access to the institute's computer systems, services, campus network, and the internet.

a. Accounts and Passwords

Users of a Net Access ID must guarantee that their ID will not be shared with anyone else. The Net Access ID should primarily be used for educational or official purposes. Users must not share their passwords or Net Access IDs with others. Network IDs will only be issued to current students, staff, and faculty affiliated with the institute. Students, staff, and faculty who leave the institute will have their Net Access IDs, email accounts, and associated files deleted. No user is permitted to hold more than one Net Access ID at a time, except for faculty or heads with multiple portfolios, who may have IDs related to their respective functions.

b. Limitations on Resource Use

On behalf of the institute, the System Administrator reserves the right to disable the Net Access ID of any user who is deemed to be using an inordinate amount of storage space or whose actions otherwise limit the availability of computing resources for other users.

c. Data Backup, Security, and Disclaimer

The System Administrator is not liable for the loss or corruption of data on individual users' computers due to the use or misuse of computing resources (hardware or software) or any damages resulting from advice or actions taken by System Administrator staff in assisting users with network or computer-related issues. Although reasonable attempts will be made to ensure data integrity, security, and privacy, users are fully responsible for backing up files in their assigned Net Access ID storage space and email accounts. Additionally, the System Administrator makes no guarantees regarding the security or privacy of users' electronic messages.

Users agree to be held liable for the improper use of equipment or software, including copyright violations, and agree to defend, indemnify, and hold the System Administrator and the institute harmless from any such liability or expenses. DB Jain retains the right to change or update these policies as necessary without prior notification to users.

d. Account Termination and Appeal Process

Accounts on Dhanraj Baid Jain College network systems may be terminated or disabled with little or no notice for the reasons stated above or for other inappropriate uses of computing and network resources. If a user believes such termination is unwarranted or that there are mitigating circumstances for their actions, they may approach the In Charge of the Computer Centre to justify why the action should not have been taken.

Writing an Appeal Letter

An appeal letter is written when you feel you have been treated unfairly and wish for someone to reconsider a decision made about you. In your letter, ensure you:

- Know the appropriate recipient
- Use a polite tone
- Clearly state what outcome you desire
- Stick to factual information, avoiding emotional language
- Follow up as necessary