INFORMATION TECHNOLOGY (IT) POLICY

MIRI PIRI KHALSA COLLEGE

BHADAUR (BARNALA)

Managed by Shiromani Gurdwara Parbandhak Committee, Sri Amritsar Sahib
Affiliated to Punjabi University, Patiala

Table of Contents

1. Need for IT Policy

The computing resources at Miri Piri Khalsa College, Bhadaur, support educational, instructional, research, and administrative activities. This policy ensures the legal and appropriate use of the Information Technology (IT) infrastructure on campus.

1.1 Objectives of the IT Policy

- **Confidentiality**: Protects sensitive data from unauthorized access.
- **Integrity**: Ensures data accuracy and consistency.
- **Availability**: Keeps IT resources accessible when needed.
- **Compliance**: Adheres to legal and regulatory requirements.
- **Security**: Protects IT resources from cyber threats and misuse.

1.2 Scope of the Policy

This policy applies to all students, faculty, staff, contractors, and visitors can access or use the college's IT resources, including:

- Computers and peripherals
- Network devices (wired/wireless)
- Internet access
- Official websites and web applications
- Email services
- Data storage systems
- Learning Management Systems (LMS)
- Multimedia and surveillance systems

1.3 Stakeholders

The policy applies to:

- **Students**: Undergraduate and postgraduate students.
- **Faculty**: Teaching and non-teaching staff.
- **Administrative Staff**: Technical and non-technical personnel.
- **Higher Authorities**: College administrators (SGPC) and officers.
- **Guests**: Authorized visitors and visiting faculty.

1.4 Policy Enforcement

Violations may result in disciplinary action, including suspension of access to IT resources. Legal action may be taken in severe cases.

2. IT Hardware Installation Policy

2.1 Primary User Responsibility

- The primary user is responsible for hardware in their assigned location.
- For shared computers, the department head designates a responsible person.

2.2 Warranty and Maintenance

- Computers must have a 3-year on-site comprehensive warranty.
- After the warranty period, an Annual Maintenance Contract (AMC) must cover repairs.

2.3 Power and Network Connections

- Computers and peripherals must connect to a UPS.
- Network cables must be kept away from electrical equipment.

2.4 File and Print Sharing

- File and print sharing must be enabled only when necessary.
- Shared files must be password-protected.

2.5 Shifting Computers

- Computers must not be relocated without informing the Network Unit.

2.6 Non-Compliance

- Non-compliance may result in network issues or disciplinary action.

3. Software Installation and Licensing Policy

3.1 Licensed Software

- Only legally licensed software is allowed.
- Pirated software is strictly prohibited.

3.2 Free and Open Source Software (FOSS)

- The college encourages FOSS to reduce costs.
- Examples include Linux and Moodle.

3.3 Operating System Updates

- Systems must be regularly updated with patches.

3.4 Antivirus Software

- Antivirus software must be installed and updated regularly.

3.5 Data Backup

- Regular data backups must be maintained on external or cloud storage.

3.6 Non-Compliance

- Non-compliance may result in data loss and disciplinary action.

4. Network Use Policy

4.1 IP Address Allocation

- IP addresses are allocated by the Internet Unit.

4.2 DHCP and Proxy Configuration

- Unauthorized DHCP or proxy settings are prohibited.

4.3 Running Network Services

- Departments must inform the Internet Unit before running network services.

4.4 Wireless Networks

- Wireless networks must be registered with the Internet Unit.

4.5 Internet Bandwidth

- All bandwidth must comply with college security policies.

5. Email Account Use Policy

5.1 Primary Use

- Email accounts are for academic and official purposes.

5.2 Prohibited Activities

- Sending spam or phishing emails is prohibited.

5.3 Data Security

- Suspicious emails or attachments must not be opened.

5.4 Non-Compliance

- Violations may result in account suspension.

6. Website Hosting Policy

6.1 Official Pages

- Official web pages must follow the college's guidelines.

6.2 Personal Pages

- Personal pages must not violate laws or host commercial content.

7. College Database Use Policy

7.1 Data Ownership

- The college owns all institutional data.

7.2 Data Access

- Data access is restricted to authorized personnel.

7.3 Data Tampering

- Data tampering may lead to disciplinary action.

8. Responsibilities of Internet Unit

8.1 Network Operations

- The Internet Unit manages the network backbone.

8.2 Network Expansion

- Expansion is reviewed annually based on funding.

9. Responsibilities of Computer Department

9.1 Hardware Maintenance

- The department maintains college-owned hardware.

9.2 Software Installation

- Only licensed software is installed.

10. Responsibilities of Sections and Departments

10.1 User Accounts

- Departments must ensure users follow IT policies.

10.2 Network Security

- Internal networks must be secure.

11. Responsibilities of Administrative Units

11.1 Information Updates

- Administrative units must update the Internet Unit on staffing changes.

12. Guidelines on Computer Naming Conventions

12.1 Naming Convention

- Computer names must include department, serial number, and MAC address.

13. Guidelines for Running Application Servers

13.1 Server Requirements

- Servers must have updated security software.

14. Guidelines for Desktop Users

14.1 Antivirus Software

- All desktops must have updated antivirus software.

14.2 Password Security

- Strong passwords must be changed periodically.

15. Video Surveillance Policy

15.1 Camera Placement

- Cameras are placed at strategic locations with signage.

15.2 Data Retention

- Recordings are retained for 15 days before overwriting.

Thank You