

Government Engineering College, Palanpur

IT Policy

Introduction:

Government Engineering College, Palanpur provides IT resources to support the educational, instructional, research, and administrative activities of the institute and to enhance the efficiency and productivity of all stakeholders. These resources serve as tools to access and process information relevant to academic and operational tasks. This document establishes specific requirements for the use and management of all IT resources at the institute.

This policy applies to all users of computing resources owned or managed by the institute, including faculty, staff, students, external vendors, departments, and any entity accessing the institute's IT infrastructure.

The main aspects of the IT policy are to:

1. Provide continuous IT infrastructure support for laboratories, faculty, staff, students, and digital information systems.
2. Regularly maintain and upgrade systems based on life cycle and technology advancements.
3. Digitize institutional information and learning resources and provide access through the internet.
4. Maintain Sophos Firewall and software for system and cybersecurity.
5. Promote open-source software.

Privacy and Personal Rights:

1. All users must respect the privacy and personal rights of others.
2. Unauthorized access to or duplication of another user's data, email, or files is prohibited.
3. While the institute generally does not monitor content, it reserves the right to access network data with due approval from the Competent Authority.

Access to Social Media Sites from Institute's Network:

1. Use is governed by the "Framework and Guidelines for use of Social Media for Government Organizations".
2. Users must comply with applicable provisions of the IT Act 2000.
3. Users must adhere to the terms and legal requirements of each social platform.

4. Any suspicious activity must be reported to the competent authority.
5. High security settings are mandatory for all users.
6. Posting of offensive or unlawful content is strictly prohibited.
7. Confidential information must not be shared without authorization.
8. Comments harming the reputation of the institute are not allowed.

Intellectual Property:

Users must not use institute resources to infringe on any intellectual property rights, including copyrights, trademarks, patents, or trade secrets.

Software Installation and Licensing Policy:

All institute computers must have licensed software only. Pirated or unauthorized software is strictly prohibited. Open-source alternatives like Linux and LibreOffice are encouraged wherever possible.

Operating System and Its Updating:

Users must ensure operating systems are regularly updated with patches and service packs.

Backups of Data:

Users must perform regular backups of important data. Use of external storage for critical backups is recommended.

IP Address Allocation:

Devices must be assigned IP addresses by the system administrator. IP address allocation is VLAN-based and follows strict DHCP pool management. Static or unauthorized use of IP addresses is not permitted.

Use of IT Infrastructure:

1. PCs are provided in laboratories for student use.
2. Admin staff and faculty are allotted PCs with print/scan access.
3. All PCs are networked and have internet access.
4. Lab Computer Systems are connected to UPS for power backup.

5. All IT assets are covered under third-party AMC.
6. Internet speed provisioned is 100 Mbps or above for all VLANs.
7. Wi-Fi is available campus-wide for authenticated users.
8. Network access is protected via Sophos authentication.
9. Internal networks are secured using Sophos Firewall and application-level filtering.
10. A dedicated committee monitors IT infrastructure and performance.

IT Support and Complaint Management:

1. Staff complaints are to be logged via the IIMP portal.
2. Complaints are addressed based on priority and escalated as per SLA.
3. A complaint tracking system is maintained for transparency and resolution.

Annual Maintenance Contracts (AMC):

Third-party AMC is in place for maintenance of:

- Computers & Printers
- Campus Wide Area Network (CWAN)
- CCTV Surveillance
- Projectors and AV Equipment

AMC vendors are responsible for preventive maintenance, fault repair, and reporting to the institute.

Policy Review and Governance:

The IT Policy will be reviewed annually or as needed by the IT Committee and approved by the Principal. Any updates will be communicated through official channels.

Enforcement:

Violations of this policy may result in disciplinary action, including termination of access, official warning, or legal recourse under the IT Act 2000 and applicable laws.