E.G.S. PILLAY ENGINEERING COLLEGE

(An Autonomous Institution Affiliated to Anna University, Chennai | Approved by AICTE, New Delhi)
(Accredited by NBA T1 (B.E. – CIVIL, CSE, ECE, EEE, MECH & B.Tech – IT)
(Accredited by NAAC with A++ Grade | One among Top 300 Engineering Institutions in India (NIRF-24)
Old Nagore Road, Thethi, Nagore Village, Nagapattinam – 611002, Tamil Nadu, India

IT POLICY

The purpose of the IT Policy in the context of the College can be summarized as follows:

1. **Maintain Security and Legal Compliance**: Ensuring the security, legal, and appropriate use of the information technology infrastructure provided by the College on campus.
2. **Protection of Information Assets**: Establishing strategies and responsibilities for the protection of the information assets that are accessed, created, managed, and/or controlled by the College.
3. **Guidance for Stakeholders**: Acting as a guide for stakeholders (students, faculty, staff) regarding the usage of the College's computing resources, including hardware, software, email, information resources, and internet access facilities.
4. **Clarifying Acceptable and Prohibited Actions**: Providing direction on what is acceptable behaviour and outlining prohibited actions or violations of policy, ensuring all users understand the consequences of misuse.

This policy ensures a safe, legal, and responsible digital environment for all members of the College.

The **Scope of the IT Policy** outlines the areas and individuals it covers, as well as the resources and activities to which it applies. Here's a breakdown:

1. **Applicability to College Technology**:
   - The policy applies to all technology administered by the College, whether centrally or by individual departments.
   - It also covers information services provided by the College administration or departments, as well as any services provided by individuals within the College community.
2. **Resources Administered by Departments**:
   - The policy extends to resources managed by various departments, including the Library, Computer Labs, Laboratories, and Administrative Offices of the College.
3. **Personal and Research Computers**:
   - Computers owned by individuals (faculty, students, staff) or those used for research projects are subject to the College IT policy when connected to the campus network.
4. **Compliance for All Users**:
   - The IT policy applies to all faculty, students, staff, departments, authorized visitors, and visiting faculty who are granted access to the College's IT infrastructure. Everyone must comply with the policy's guidelines.
5. **Key Areas of Focus**:
   - **IT Hardware Installation and Maintenance**: Guidelines for how hardware should be installed and maintained.

- **Software Installation and Licensing**: Policies on software installation and compliance with licensing laws.
- **Network (Intranet & Internet) Use**: Guidelines for using the College's network, both internal (intranet) and external (internet).
- **E-mail Account Use**: Proper use of the College's e-mail system.
- **Web Site Hosting**: Policies around hosting websites on College infrastructure.
- **College Database Use**: Guidelines on the appropriate use of College databases.
- **Role of Network/System Administrators**: The responsibilities of administrators who manage the network and systems.

The scope ensures that all members of the College community are aware of the standards and rules governing the use of IT resources, contributing to a secure and efficient technological environment.

The **IT Hardware Installation and Maintenance Guidelines** outline the procedures and responsibilities for handling IT hardware within the College. Here's a breakdown of these guidelines:

1. **Responsibility for Installation and Maintenance**:
   - **System Administrators** are responsible for performing IT hardware installation and maintenance.
2. **IT Hardware Requests**:
   - Faculty and departments can submit their **IT hardware requirements** based on their academic needs.
   - The **procurement of IT hardware** should be initiated considering both the stock availability and the submitted requirements from the departments.
3. **Stock Management**:
   - When new IT hardware is procured, the **Stock Register** should be updated immediately to ensure accurate tracking.
4. **Approval for Installation and Maintenance**:
   - **After Approval from the Management,** Department is required before any IT hardware installation or maintenance services are provided.
5. **Periodic Maintenance**:
   - **System Administrators** must carry out periodic maintenance of computer systems, with all maintenance activities recorded in a **Maintenance Register** to ensure proper documentation and accountability.
6. **Movement of IT Hardware**:
   - Any movement of IT hardware, either within the college or outside, must be documented in the **Movement Register** for tracking purposes.
7. **Disposal of E-Waste**:
   - Major **e-waste** (such as written-off instruments, CRTs, printers, computers, and batteries) should be sold regularly in a responsible manner to manage waste and ensure compliance with environmental standards.
8. **Responsibility for Hardware**:
   - The **Faculty or Department** is solely responsible for the IT hardware assigned to them. Any **damage, loss, or theft** of the hardware must be addressed by the respective department or faculty, and they bear the financial responsibility for such issues.

These guidelines ensure that the installation, maintenance, and management of IT hardware within the College are carried out in an organized and accountable manner, contributing to the longevity and security of the College's IT infrastructure.

The **Software Installation and Licensing Guidelines** provide clear instructions for managing software within the College. Here's a breakdown of these guidelines:

1. **Authorized and Open Source Software**:
   - The **College IT policy** permits the installation of **authorized** and **open source software** on College computers.
   - If there are any violations of this policy, the College will hold the **Department/Individual** responsible for any non-compliance.
2. **Preference for Open Source Software**:
   - **Open source software** should be prioritized and used wherever possible in College systems to promote cost-effectiveness and security.
3. **Licensed Software**:
   - All **licensed software** must be installed on systems, ensuring that all software in use is legally compliant and appropriately licensed.
4. **Antivirus Software**:
   - **Antivirus software** should be procured and installed on all College systems to protect against malware and cyber threats, ensuring the security of the IT infrastructure.
5. **Data Backup**:
   - **System administrators** must periodically back up data and store it in **External Hard Disks** to prevent data loss and ensure the integrity and security of information.
6. **Compliance with Standards**:
   - **Software used for academic and administrative purposes** should comply with **ISO standards**, ensuring that it meets quality, security, and interoperability requirements.

These guidelines are designed to ensure that the software used within the College is both legally compliant and secure, while also maintaining a focus on efficient use of resources through the promotion of open source solutions where possible.

The **Network (Intranet & Internet) Use Guidelines** provide a framework for managing the use of the College's network resources, ensuring security, efficiency, and appropriate usage. Here's a breakdown of these guidelines:

1. **IP Address Assignment**:
   - Any **computer (PC/Server)** that will be connected to the College network must have an **IP address assigned by the System Administrators** to ensure proper network management and prevent conflicts.
2. **IP Address Usage**:
   - An **IP address allocated for a particular computer** should **not** be used on any other computer, even if it belongs to the same individual or is connected to the same network port. This ensures that each device on the network is uniquely identifiable.
3. **Prohibition on Changing IP Address**:
   - It is **strictly prohibited** for staff or students to change the **IP address** of any computer. This helps prevent network conflicts and maintains proper system configurations.
4. **Network Configuration**:
   - The **configuration of the network** is the responsibility of the **System Administrators** only. Unauthorized changes could compromise network performance and security.

5. **Running Server Software**:
    - Departments or individuals wishing to connect to the College network over **LAN** and run **server software** must inform the **System Administrators** beforehand. This ensures that the network remains stable and secure.
6. **Access to Remote Networks**:
    - **Access to remote networks** via the College's network connection must comply with all policies and rules of the remote networks being accessed, maintaining security and compliance at all times.
7. **Internet and Wi-Fi Usage**:
    - **Internet and Wi-Fi facilities** should be used solely for **academic** and **administrative purposes**. This ensures that the network resources are used efficiently and for the intended purposes of the College.

These guidelines are aimed at maintaining network security, preventing misuse, and ensuring that all users of the College's network are following best practices for network management and use.

The **Email Account Use Guidelines** are designed to ensure responsible and secure usage of the College's email system. Here's a breakdown of these guidelines:

1. **Faculty Email Provision**:
    - Every **faculty member** is provided with a College **email account** for official and academic communication.
2. **Purpose of Email Use**:
    - The email facility should be primarily used for **academic and official purposes**. Personal use is allowed but should be **limited**.
3. **Prohibition of Illegal/Commercial Use**:
    - Using the email system for **illegal activities** or **commercial purposes** is a direct violation of the College's IT policy and could result in the **withdrawal of the email facility**.
4. **Privacy and Security**:
    - Faculty must refrain from **intercepting** or attempting to access others' email accounts, as this is a violation of privacy.
    - **Impersonating** another individual's email account is considered a **serious offense** under the College's IT security policy and may lead to severe consequences.
5. **Personal Responsibility**:
    - It is the **individual responsibility** of each user to ensure their email account adheres to the College's email usage policies and is free from violations.

These guidelines ensure that the College's email system is used ethically, securely, and in compliance with academic and professional standards, safeguarding both individual privacy and the integrity of the College's network.

Web Site Hosting Guidelines

1. **Purpose of the College Website**:
   - The **College website** should serve to provide **academic** and **administrative information** to stakeholders, ensuring that all content is relevant and up-to-date.
2. **Website Updation Committee**:
   - A **Website Updation Committee** is responsible for maintaining and updating the content of the website, ensuring that pages are regularly reviewed, links are tested, and content remains accurate.
3. **Content Quality**:
   - The content on the website must be **clear** and **correct**, and all pages should be proofread and links tested before being made live.
4. **Department and Association Web Pages**:
   - **Departments and Associations** (Teachers, Employees, Students) may have official web pages, but these must adhere to the **College Website Creation Guidelines** to maintain consistency and quality.
5. **Learning Management System (LMS)**:
   - The **LMS** can be linked to the website, allowing faculty to post **class materials** such as syllabi, course materials, and resources to facilitate **eLearning**.
6. **Data Security**:
   - The **Website Updation Committee** must take appropriate measures to **safeguard the security** of all data hosted on the website, ensuring that sensitive information is protected.

College Database Use Guidelines

1. **Data Protection**:
   - The **College administration** must ensure the protection of databases maintained under the College's **e-Governance** system. The College owns all institutional data generated.
2. **Custodianship**:
   - **Departments or individuals** may generate portions of data and thus may have custodianship responsibilities for specific datasets.
3. **Confidentiality**:
   - The College's data policies prohibit the distribution of **identifiable personal data** outside the institution. Data from the College's database is strictly for **internal College purposes**.
4. **Access to Data**:
   - Data access is determined by an individual's role and responsibilities. College data is made available based on **official duties/rights**.
5. **Handling Data Requests**:
   - Requests for data from outside entities (e.g., government agencies, courts, attorneys) must be **forwarded to the IQAC Office**, which handles such requests. Faculty or departments should not respond directly to these requests.
6. **Prohibition of Commercial Use**:
   - **Personal or directory information** may never be released for **commercial**, **marketing**, **solicitation**, or other non-institutional purposes.

7. **Database Tampering**:
    - **Tampering** with the College's database is considered a violation of the IT policy. Violations may lead to **disciplinary action**, and if illegal, law enforcement agencies may be involved.

Responsibilities of Network/System Administrators

1. **Network Design and Backbone Operations**:
    - System administrators are responsible for **designing the College network** and performing **backbone operations** to ensure smooth functioning.
2. **Networking and Maintenance**:
    - They handle the configuration and maintenance of **Wireless Local Area Networks (WLANs)**, classroom IT facilities, and **lab systems**.
3. **Troubleshooting and Complaints**:
    - **Complaints from users** about network issues are received and addressed by the system administrators.
4. **Server and Hardware Maintenance**:
    - The administrators maintain servers, computer hardware, peripherals, and networking devices to ensure operational efficiency.
5. **Unauthorized Software Installation**:
    - Administrators must **discourage the installation of unauthorized software** on any computer system within the network and refrain from accommodating such requests.

E-Waste Management

1. **E-Waste Initiatives**:
    - The College has taken proactive steps for **eco-friendly** e-waste management, ensuring that electronic goods are put to **optimum use**. Minor repairs are done by staff, and major repairs are handled by the **Technical Assistant**.
2. **Redistribution**:
    - **Old computers** and **LCD projectors** are transferred to schools run by the College's education society for reuse.
3. **E-Waste Disposal**:
    - Major e-waste, such as **written-off instruments, CRTs, printers, and computers**, is sold off regularly.
4. **Battery Management**:
    - **UPS batteries** are recharged, repaired, or exchanged by the suppliers to ensure continued usability.
5. **Safe Disposal**:
    - Miscellaneous e-waste, such as **CDs**, **batteries**, **fluorescent bulbs**, and other non-hazardous items, are safely collected from departments and disposed of properly.
6. **Student Involvement**:
    - Students are encouraged to use waste **CDs and other non-hazardous items** for creative projects like **decorations**.
7. **Awareness Programs**:
    - The College conducts **awareness programs** to educate students on **e-waste management** techniques, promoting sustainable practices.

These guidelines ensure that the College's IT resources are used responsibly, promoting security, sustainability, and ethical practices while safeguarding both data and the environment.