IT Policy

MAR ATHANASIUS COLLEGE(AUTONOMOUS)

Mar Athanasius College(Autonomous) maintains an IT policy that promotes the optimum use of IT resources in the college. It intends to achieve a systematic mechanism for the use of IT resources for students, research scholars, staff and faculty members.

Information technology policies articulate the institution's vision, strategy, and principles. The IT policies interpret applicable laws and regulations and ensure that the policies are consistent with legal and contractual requirements. In addition, IT policies specify requirements and standards for the consistent use of IT resources within the Institution.

A senior faculty is appointed as IT Coordinator and two IT staffs are appointed to assist him. The purpose of this policy is to detail the acceptable use of information technology resources for the protection of all the concerned parties involved. The scope of this policy includes the use of institutional IT resources, including but not limited to, computer systems, email, the network, and the Internet connection. The policy outlines the email use, confidentiality, social media and web browsing. Network usage inside the campus is protected by password and an affidavit is to be signed by the students to get the password.

Software

·   Based on the directions from Kerala Government and the University, the systems are mainly working on open-source software.

·   The institution reserves the right to limit, control, restrict and reject access to institutional data and information sharing.

·   Data and software are protected using authentic, paid antivirus package and fire walls.

Wireless Network

Wireless access shall be done securely through certain steps to mitigate known risks. Access to wireless network is protected by password for staff and students. Social media is blocked for students during working hours. Guest access to the institutional network is often necessary for students, customers, consultants, or vendors who are visiting the Institution. Guests can access the network with permission.

Network Security

·   Institution needs a secure network infrastructure to protect the integrity of its data and mitigate risk of a security incident. The purpose of a specific network infrastructure security policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure.

·   This policy might include specific procedures around device passwords, logs, firewalls, Networked hard wares, and security testing.

MAR ATHANASIUS COLLEGE(AUTONOMOUS)

Mar Athanasius College(Autonomous) maintains an IT policy that promotes the optimum use of IT resources in the college. It intends to achieve a systematic mechanism for the use of IT resources for students, research scholars, staff and faculty members.

Information technology policies articulate the institution's vision, strategy, and principles. The IT policies interpret applicable laws and regulations and ensure that the policies are consistent with legal and contractual requirements. In addition, IT policies specify requirements and standards for the consistent use of IT resources within the Institution.

A senior faculty is appointed as IT Coordinator and two IT staffs are appointed to assist him. The purpose of this policy is to detail the acceptable use of information technology resources for the protection of all the concerned parties involved. The scope of this policy includes the use of institutional IT resources, including but not limited to, computer systems, email, the network, and the Internet connection. The policy outlines the email use, confidentiality, social media and web browsing. Network usage inside the campus is protected by password and an affidavit is to be signed by the students to get the password.

Software

·   Based on the directions from Kerala Government and the University, the systems are mainly working on open-source software.

·   The institution reserves the right to limit, control, restrict and reject access to institutional data and information sharing.

·   Data and software are protected using authentic, paid antivirus package and fire walls.

Wireless Network

Wireless access shall be done securely through certain steps to mitigate known risks. Access to wireless network is protected by password for staff and students. Social media is blocked for students during working hours. Guest access to the institutional network is often necessary for students, customers, consultants, or vendors who are visiting the Institution. Guests can access the network with permission.

Network Security

·   Institution needs a secure network infrastructure to protect the integrity of its data and mitigate risk of a security incident. The purpose of a specific network infrastructure security policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure.

·   This policy might include specific procedures around device passwords, logs, firewalls, Networked hard wares, and security testing.

· Institutional personnel may not broaden access to institutional data without authorization from the Management. This limitation applies to all means of copying, replicating, or otherwise propagating institutional data. Authorization to access institutional data varies according to its sensitivity. It's important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability. The need for integrity or trustworthiness, of institutional data shall be considered and aligned with institutional standards. Unauthorized use / modification of institutional data invite disciplinary / legal action. The institution is committed to provide quality IT services by constant upgrading of facilities and introduction of latest updated software.

Duties of IT Coordinator

· Administration and maintenance of the common facilities such as Central Computer Center, LAN and WiFi networks in the campus.

· Identify failures in Campus network and rectify it.

· Make arrangements for online examinations, Training and Placement tests and training programmes of external agencies (approved by the management).

· Monitor the data usage and warn/terminate the unauthorised usages if any.