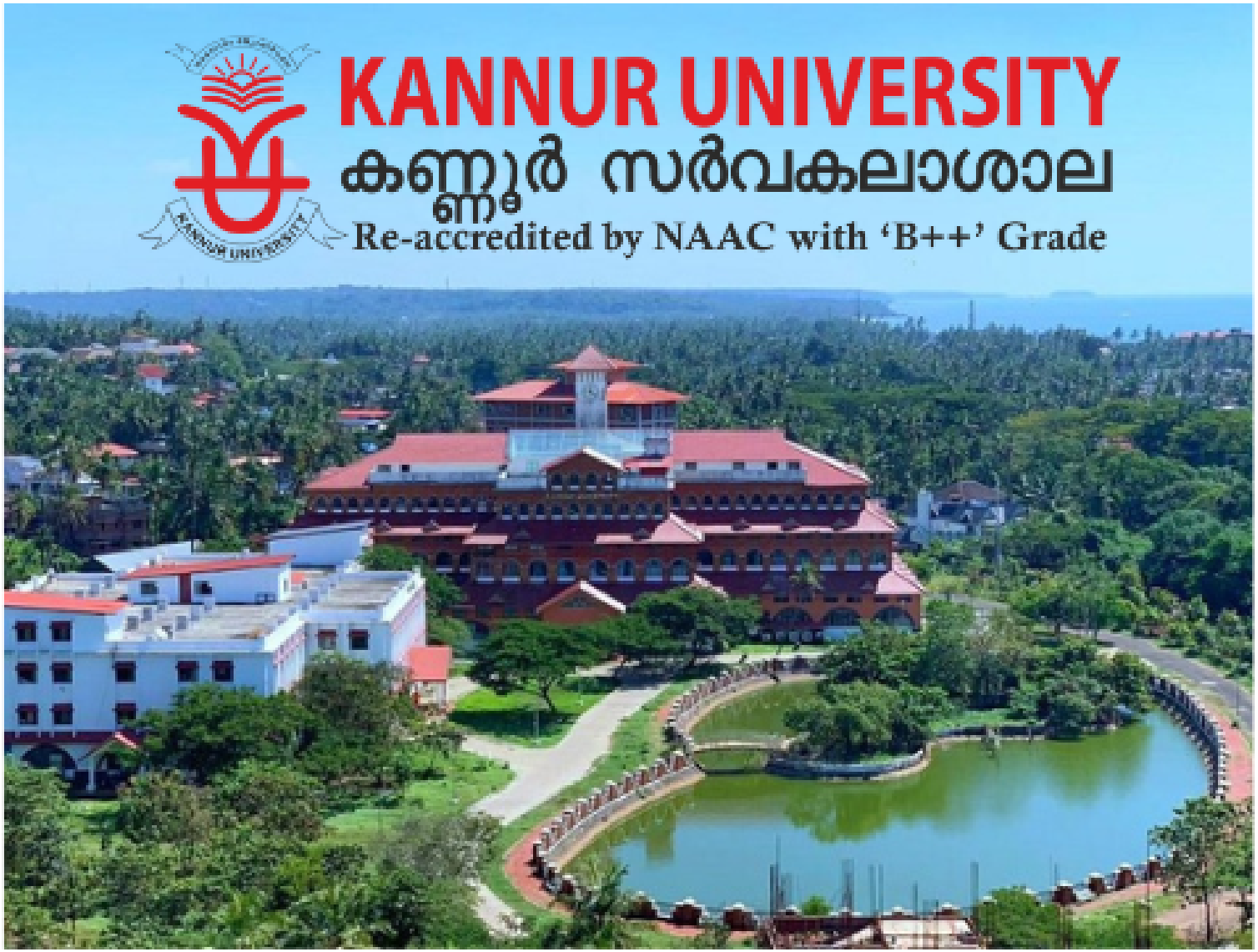
KANNUR UNIVERSITY
കണ്ണൂർ സർവകലാശാല
Re-accredited by NAAC with 'B++' Grade

Information Technology (IT) Policy

Kannur University

Kannur University Information Technology (IT) Policy govern the responsible usage of all users of the University's information technology resources.

Kannur University Information Technology (IT) Policy

Kannur University Information Technology (IT) Policy govern the responsible usage of all users of the University's information technology resources. This comprises the IT facilities allocated centrally or by individual departments. Every member of the University is expected to be familiar with and adhere to this policy. Users of the campus network and computer resources ("users") are responsible to properly use and protect information resources and to respect the rights of others.

Applicability of Policy

Scope of this policy covers purchase, maintenance and disposal of IT equipments and services of University offices and departments. Also applicable for all staff members and all other stake holders of the University system.

Security Auditing policy

At least every 5 year; security auditing of IT equipments, software and services and internet security shall be done using the expertise of an empanelled agencies of Central/ state government Agencies.

Website policy

- Official website should be hosted @ state data centre.
- Development, administration and maintenance of official website and portals are the responsibilities of IT Centre
- Technology upgrading security auditing shall be done as and when required as per the directions of Central / state Government agencies.
- Contents to be updated/ removed shall be forwarded by concerned offices and departments through office of the Public Relations Officer

Software Development Policy

- System development should be done by right trained developer in order to ensure best Quality of the delivered outcome

- System development includes all digital development activities like software development, application development, mobile application development, workflows development, website development etc.
- Source code should be securely saved and kept with a proper versioning, description and documentation
- A proper design and requirements specifications must be documented (SRS).
- A proper stakeholder's acceptance and sign off should be done by the of development phase.
- Developers shouldn't operate or maintain the developed system. It should be handed over to application administrators/Maintenance Team with proper day to day running manuals.
- Proper vulnerability and patch management should be performed for any developed system.
- No unknown source codes, functions, libraries or APIs are allowed to be used in system development.
- All related processes and development activities must be documented and saved for future reference.

IT Hardware Policy.

Purchase Procedure

The entire hardware requirement from the Teaching Department and Non-Teaching will be processed by the purchase sections and after getting approval from the higher authorities it will be forwarded to the IT Cell for the further proceedings. IT Cell then prepares the specification and estimate amount of the same and also ensures the maximum support in the tender proceedings.

System Service

- All the system maintenance works are carried out by the IT hardware wing.
- Prior intimation and permission is required for shifting of Hardware items from one section to another.
- Users are restricted to work on the allocated system only.

Server Policy

Kannur University is keen to provide servers with maximum configuration. Every time the new server is available, it is shifted as an online server for providing high speed service to the online users.

Kannur University always keeps at least one server as standby for handling the unexpected shutdown of a working server. The service of the troubled server may be reinstating within a short span of time. Urgent action may be initiating as early as possible for the service of the troubled server.

Network and Internet Policy

- Primary purpose of the network policy is to inform users and staff about the requirements for protecting the various assets of the organization such as passwords, critical databases, vital applications, shared storages, confidential documents, servers etc.
- Firewall used in the Kannur University is the first line of defence and the cornerstone of its security. Hence it supports a strong and dynamic security policy. Firewall is purchased with a 3 year license subscription and with a 300 concurrent user license.
- Kannur University has an Internet bandwidth from NKN and of Bandwidth availability 1 Gbps. This connection is distributed to all the campuses through point to point connectivity through BSNL.
- The Hardware wing in the IT Cell is responsible for the maintenance and support of the Network such as Assigning and revoking privileges, Disaster Recovery, Acceptable Use, Back Up, Archiving and fail over policies.

IT Email Policy

An Email Policy ensures to implement each user to use their email in a way that is assigned and aligned with the aim of the institution. That way an Email Policy will help ensure that users/staffs are aware of their responsibilities when using the email service.

General Guidelines includes,

- Choose a Strong Password.
- Update your password at a regular time period.
- Never hand out your mail password.
- Do not write down your password
- Verify the legitimacy of each email, including the email address and sender name.
- Avoid clickbait titles and links. [Do not click attachments, or links on unsolicited emails especially from an unknown person/source.]
- Kannur University official email id uses, kannuruniv.ac.in as the e-mail domain.

  For example vc@kannuruniv.ac.in, registrar@kannuruniv.ac.in

Violation of Policy:

Any violation of the basic objectives and areas mentioned under the IT Policy of the University shall be considered as a violation and as a misconduct and gross misconduct under University Rules.

Implementation of Policy:

For implementation of this policy, the University will decide necessary rules from time to time.

Review and Monitoring:

The Policy document needs to be reviewed at least once in two years and updated if required, so as to meet the pace of the advancements in the IT related development in the industry.