Madurai Kamaraj University

(University with Potential for Excellence)

Re-accredited by NAAC with 'A' Grade in the 3rd Cycle

COMPREHENSIVE INFORMATION TECHNOLOGY (IT) POLICY

Madurai Kamaraj University provides its Faculty Members, Research Scholars, Staff and Students various IT services like Internet, Automation of University activities etc. It is essential to device an IT Policy to regulate the users for receiving well organized IT services. These policies must be pertinent exclusively for Madurai Kamaraj University which is flexible as well as protected.

Information Technology Policies need to be specified for the following major factors:

- Regular Activities;
- Infrastructure;
- Software;
- Network (Internet & Intranet) and
- Web Site Management

Regular Activities

Following major units are using IT facilities of University.

- University
  - ❖ Administration (Establishment, Examination, Finance etc.)
  - ❖ Academic (Schools/ Departments / Centres)
  - ❖ Library
- Directorate of Distance Education

Infrastructure

Infrastructure development, usage and maintenance are the common activities of the entire University. Every year all the Schools/Centres/Administrative wings take steps to augment the existing infrastructure as the need grows.

Hardware

- Purchase of any IT products must strictly follow the Government policies that are currently pursued.
- Any IT product must be procured only from authorized dealers, who produce authorization letter from the respective companies, preferably using DGS & D Rate Contract.
- Every Hardware purchased must be properly installed by the certified Engineers and duly produce Installation Certificate after running a Bench Mark test.

- Power connections sources must be properly completed before the installation by authorized persons. The ISI quality products only must be used for providing the connection. Proper earth must be constructed and tested before using the product.
- Necessary spike busters and surge control equipments must be part of the constructing the electrical work.
- After expiration of warranty /AMC period a new Annual Maintenance Contract may be executed within a time period not exceeding two weeks.
- As part of purchase, due training must be imparted to staff of the University, who will be responsible for the product.
- IT products like Computers etc found to be obsolete but
    - usable, can be donated to requiring uses;
    - not usable, can be condemned by a central pool with proper records.

Software

- Users must be encouraged to use open Sources software than proprietary software. Necessary awareness can be brought to all sections of users by a team who has expertise in using Open sources.
- Any proprietary software must be used only after purchasing with proper license.
- Usage of unlicensed software is strictly prohibited.
- After expiration of Warranty/ AMC period, a new Annual Maintenance Contract should be executed to avoid inactivation.
- Any software, which is property of the University, should not be used for commercial use
- Some softwares can be shared by other school/ department / centre/ any administrative wing on genuine demand without any violation.

Networking (Internet / Intranet)

Internet

- A network Management Team (NMT) is responsible for providing Internet service to all users of University.
- Users Ids must be provided to use Internet by (NMT) and due records must be provided.
- For students, validity period of usage must be based on the course. At the end of the course, the User IDs must be deactivated automatically.
- For Research Scholars, the User IDs can be provided till the end of the Research period mentioned in their Registration. It can be extended on request from their Research Supervisor. In any case, the User IDs must be deactivated automatically at the end of the period.
- Faculty members must be encouraged to use official email id.
- Faculty members retiring must be permitted to use the Internet facilities at least for one year on obtaining due permission from Registrar.
- Students must product No Dues Certificate from NMT at the time of leaving.

Usage

- Users are restricted to download and store offensive materials in the common storage media.
- Should not play games during Lab sessions.
- Recreational downloads in common lab is strictly prohibited.
- Spamming strictly prohibited.
- Sending emails harassing, offending, abusing or any other illegal form is an offence. If brought to the notice with evidence, severe action will be taken.
- Users can use only official University Wi-Fi network for their wireless needs. Setting up unsecured Wi-Fi on campus is strictly not allowed. Such set ups should not interfere with the bandwidth of university provided bandwidth.
- Students using removable media (pen drives, data cards and readers, Floppies, writable CDs etc) must be restricted.

Protection

- Firewalls must be installed and properly maintained at Network Management Centre. Current updates must be duly carried out. The firewall must meet the International standards so that any item passing through this firewall does not affect the internal resources on campus.
- Antivirus software must be installed and maintained by the users at their own cost.
- Any hacking or attempt to hacking both Internal / External is an offense. Any tool used for hacking resources of university or any other should not be installed in any system in the campus.
- It is not possible to disclose all the matters of the University publicly. Matters that are disclosed must be properly analysed and due permission must be obtained from the concerned authorities.
- Users IDs allocated to individual users should not be shared with others. Especially for Wi-Fi connectivity, it is the responsibility of the individual to maintain their Used Id and Password as confidential and the risk of disclosing the same will be met by the individual.
- Any unauthorized attempt to modify University resources (like Data Bases etc) is an offence. Such resources can be highly protected and inaccessible by users. If accessible, it must be under 'Read only' with due permission.
- Impersonating others email accounts is treated as serious offense.

Website Management

- University website must be duly maintained by a Web Administrator and a team
- It should be protected sufficiently from external used with tamper the content of the Website like "Dynamic Pages".
- Periodic updates of the website are done with due care.

* * * * *