IT POLICIES AND PROCEDURES

(Approved by BOG)

INFOCELL

K.L.E. TECHNOLOGICAL UNIVERSITY, HUBBALLI

INFOCELL

Information Technology Policy

Table of Contents

Introduction

The KLE Technological University, from its inception in the year 2015, has IT Policy, which provides the policies and procedures for the selection and use of IT infrastructure within the campus. All the employees and students must follow the Policy.

KLE Technological University will keep all IT policies current and relevant. Therefore, from time to time, it will be necessary to modify and amend some sections of the policies and procedures.

Any suggestions, recommendations, or feedback on the policies and procedures specified in this are welcome.

These policies and procedures apply to all employees and students.

The policy is approved by the Board of Governance (BoG).

KLE Technological University has an extensive and comprehensive policy to bring radical changes in ICT implementation in the fast-changing technological scenario.

The Information Services Cell (Infocell) of the university has been assigned the responsibility to develop and manage the IT- infrastructure and services for the university. Infocell is headed by a faculty Coordinator and supported by a technical team. Infocell has formulated and monitoring IT service management policies for the university. IT service management policies of the university is classified into the following groups:

1. IT Security Policy.
2. Email policy.
3. IT Data Backup policy.
4. Software purchasing policy.
5. Hardware purchasing policy.
6. Policy for the use of Software.
7. IT Procurement Policy.
8. Bring your own device policy.
9. E-waste Policy

1 Policy for the use of Software

Policy Number: 1.0

Policy Date: 11-09-2020

1.1.1 Purpose of the Policy

This Policy provides guidelines for software use for all employees within the campus to ensure that all software use is appropriate. Under this Policy, FOSSEE software will be conducted under the same commercial/educational software procedures.

1.1.2 Software Licensing

All employees of the campus will follow all computer software copyrights and terms of all software licenses.

Where licensing states limited usage (i.e., number of computers or users, etc.), it is the IT cell's responsibility to ensure these terms are followed.

The Department lab instructor is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and license agreements have adhered.

1.1.3 Software Installation

KLE Technological University is to be the registered owner of all software.

Only software obtained in accordance with the getting software policy is to be installed on the campus’s computers.

All software installation is to be carried out by the lab instructor in coordination with IT Cell.

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software, and necessary application software) installed. Respecting the country's anti-piracy laws, University IT policy does not allow any pirated/unauthorized software installation on the university-owned computers and the computers connected to the University campus network. In the absence of

such undertakings, University will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individual rooms.

1.1.4 Software Usage

Only software purchased in accordance with the getting software policy is to be used within the campus.

Before using any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on the use of the software.

All employees must receive training for all new software. It includes new employees to be trained to use existing software appropriately. This will be the responsibility of the lab instructor / IT Cell.

Employees and students are prohibited from bringing software from home and loading it onto the campus's computer hardware.

Unauthorized software is prohibited from being used on the campus. This includes the use of software owned by an employee and used within the campus.

The unauthorized duplicating, acquiring, or use of software copies is prohibited. Any employee who makes acquires or uses unauthorized copies of software will be referred to The Registrar for disciplinary action. The illegal duplication of software or other copyrighted works is not condoned within this campus, and The Registrar is authorized to undertake disciplinary action where such event occurs.

2 IT Security Policy

Policy Number: 2.1

Policy Date: 10-09-2020

At KLE Technological University, we acknowledge the importance of the security of information.

2.1.1 Purpose of the Policy

This Policy ensures the user of KLE Technological university secured data access across the campus.

2.1.2 Password Policy

Staff and student of the university will be using numerous accounts across campus.

- Official university e-mail ID
- Microsoft Teams ID for online classes.
- Student & Staff management (contineo)
- Matlab account.
- Network authentication.
- Elearning library contents.
- Learning Management System (LMS)

All these accounts are password protected. A firm password policy ensures that the student and staff should change the one-time password at first login. It also ensures that the mobile number and alternative email id is registered for a password reset.

2.1.3 Network Security Policy

A high-end industry-standard firewall monitors the data access across campus. A usage log report is maintained on a regular basis. Access point controller unit and AAA server govern data security across campus wifi and lan.

All the desktop servers and workstations, and university laptops are installed with endpoint security software (antivirus).

Antivirus Software and its updating: Computer systems used in the University should have antivirus software installed, and it should be active at all times. The primary user of a computer

system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from lab instructor.

2.1.4 Network VLAN Policy

IP Address Allocation: Any computer (PC/Server) connected to the University network should have an IP address assigned by the Infocell. Following a systematic approach, the range of IP addresses allocated to each building is via a dedicated VLAN. This centralized DHCP server takes care of IP allocation and leases time. When a new server is installed and requires a static IP the concerned user can approach Infocell for a Static IP address.

DHCP and Proxy Configuration by Individual Departments / Users: Use of any computer at end-user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered an absolute violation of IP address allocation policy of the University. Similarly, the configuration of proxy servers should also be avoided, as it may interfere with the service run by Infocell.

VPN: The Virtual Private Network access given with prior permission.

High-security zones like the exam section, account section, and data centers have biometric entry. In these areas, trespassing is monitored on CCTV.

Exam section LAN is isolated from accessing from campus LAN.

3 Email Policy

Policy Number: 3.1

Policy Date: 10-09-2020

Recognizing the advantages of effective email service for its Staff and students, the KLETU, through the Information Services Cell(InfoCell). Factors taken into account in this will include:

- scalability of email system;
- integration with standard desktop environment across multiple platforms;
- compatibility with other systems in use across the Internet;
- feature rich;
- powerful administrative interfaces;
- accessible via browser interface;
- spam free
- supports pop3 and imap

3.1.1 Purpose of the Policy

This Policy provides guidelines to create and use of KLE Technological University email.

3.1.2 Access to the KLETU Email Environment

Access to the KLETU environment shall be available to all users with authorized accounts as specified in the Acceptable Use of IT policy. Access shall be available through local on-campus or remote off-campus means.

KLETU facilities are not to be used for commercial purposes other than those which are directly related to the business of the KLETU.

3.1.2a Applying For An Email Account (Staff)

An applicant for an email account should download the application form from infocell.kletech.ac.in, obtain the appropriate signature and forward the completed original form to the IT Help Desk.

3.1.2b Applying For An Email Account (Students)

For all the students of KLETU email account is automatically created as part of the enrolment process.

3.1.2c Gaining Access (Staff)

Use of the email client (such as outlook or thunderbird) installed on a staff desktop machine is the preferred method of access. This is the fastest, easiest, and most comprehensive method for accessing email. Every staff desktop computer should have the email client software installed on the machine.

An alternate method is to use a web browser to access the email account via a web browser. This method is best used within the KLETU when Staff is at a different location from their staff desktop machine, as it provides for simple access to email. Further details on accessing email on the web are found at the Outlook Web Access Help Pages

3.1.2d Gaining Access (Students)

When on campus, students can use the email client installed in student computer pools, or access their email via web browser.

3.1.3 Responsibilities of Use of KLETU Email Facilities

Each person who has access to the email facilities provided by the KLETU has the responsibility to use those facilities according to the Acceptable Use of IT policy.

3.1.4 On-line Mailbox Space Management

The mailbox space is unlimited for students and Staff.

3.1.5 Usernames and Passwords

The InfoCell will assign a Username and Password for each person given access to the KLETU Technology email facilities. Users may change their passwords at any time.

Username and passwords are subject to guidelines defined in the Username and password policy. InfoCell has the responsibility for assigning an email address to an appropriate username.

The IT Acceptable Use policy provides additional guidance on user accounts and passwords.

3.1.6 Format of Staff and Student Email Addresses

3.1.6a Staff

Staff will have an email address of the format: firstname.lastname@kletech.ac.in

In some cases, alternative forms of email address may also be assigned to Staff, such as nickname.lastname@ kletech.ac.in

In the case of staff members with the same name, a middle initial will be used to differentiate the two users, such as firstname.middleInitial.lastname@ kletech.ac.in

Staff email addresses of the form abbreviation.lastname@ kletech.ac.in and anyname@org-code. kletech.ac.in will no longer be created. Some existing addresses of this form which are heavily used will be maintained until the staff member leaves.

3.1.6b Students

Students will have an email address of the format: Mail-ID@ kletech.ac.in

The Mail-ID of a student will be in the form 01feXXbXXNNN, where

- 01fe = the full time engineering.
- 19 =the two digits of student year of admission.
- XXX=the three digits of student branch
- NNN =three digits starting at 001 for the first student with a particular combination of letters and incrementing by one for each subsequent student with the same combination of letters.

3.1.7 Deleted Accounts

3.1.7a Procedures relating to email when a staff member leaves

- When a staff member's email account is to be deleted because they leave the KLETU, the person requesting the deletion must complete the appropriate form and have it authorized by the relevant Head of Department.

- It is the responsibility of the departing staff member to tidy up their email account before their departure. Messages which relate to KLETU business should be retained or archived appropriately. Messages which remain in the email account will be viewed by other Staff once the departing staff member has left or can be delegated to another staff member.

- Deleted email accounts remain active for three months. During this time all email addressed to the mailbox is redirected to the member of Staff who requested the deletion or their delegate. This person then has the responsibility for managing that mail.

- New messages which arrive for a deleted email account in the three-month period will not be automatically redirected to an email account external to the KLETU. Personal mail messages for the former staff member will be on forwarded (if a forwarding e-mail address is known) on the request of the departing staff member. KLETU e-mail messages will not be disclosed nor forwarded to the former staff member.

After three months, the entire mailbox for the former staff member will be archived and then deleted from the address book.

3.7.1b Students

Student email accounts will normally be disabled or deleted at the end of the final semester.

3.1.8 Use of Email Signatures

3.1.8a Include a signature file on all e-mail

The signature can be added with appropriate syntax

Do not include drawings, pictures, maps, graphics in your signature or an inspirational or another type of quotation at the end. Such material is unnecessary in business communication and may not be well-received.

4 IT Backup Policy

Policy Number: 4.1

Policy Date: 10-09-2020

At KLE Technological University, we acknowledge the importance of data and its accessibility. Data that is generated has many formats, for example, staff data, student's data, and library data, etc.

4.1.1 Purpose of the Policy

This Policy provides guidelines to the laboratory staff or instructors and IT Admin to make the most use of appropriate data and its backup procedures.

4.1.2 Backup Procedure and Policy

- Student's files are stored safely on the system running Windows 2012 server OS which is configured as Active Directory Server/ File Server. Each user is allocated with a unique login ID & password, with respect to every login ID a folder is created, where the user with that particular Log-In ID has to store his/her files in the respective folder only. The access to the particular folder is restricted to the Log-In ID with a password and to the administrator only.

- The lab instructor creates valid Login IDs of all the students. The log-In ID of students is their respective University Seat Numbers. e.g. 01fexxbxxxxx

- A disk quota of 150 M.B with variable space is enabled for student accounts on the server.

- A user can login on to any machine. While logging, he/ she has to choose a domain name. On successful Login, he/she has access to all the resources of the local machine and also to his/her Network folder on the server (access to which can be through an icon displayed as Z:drive in My Computer on the local machine)

- The user folders on the ADS server are backed up daily at 5:30 P.M on a local drive. And a permanent copy is maintained on external hard drive at the end of the semester. The above task is performed by the backup operator. By doing so, we can assure maximum safety of the user data.

- The backup on the external hard drive is kept or trashed as per the respective department head's decision.
- The Passwords of all the systems to be changed once in a fortnight by the Administrator. Also, a hard copy containing the same is sealed in a cover & submitted to the HOD. The previous hard copy containing the passwords needs to be destroyed.
- All the servers and workstations are enabled with RAID.
- Configuration and data backup of Firewall, Access Controller unit, and Antivirus is automatically carried out daily at 4:15 PM and mailed to the administrator email ID.
- Student admission/ course registration/ attendance/ fees/ exam all data is stored at the contineo server and replicated on the cloud.

5 Software Purchasing Policy

Policy Number: 5.1

Policy Date: 11-09-2020

Purpose of the Policy

This Policy provides guidelines for the campus purchase of software to ensure that all campus software is appropriate, value for money, applicable, and integrates with other campus technology. This Policy applies to software obtained as part of a hardware bundle or pre-loaded software.

Procedures

5.1.1 Request for Software

All software, including types of non-commercial software such as open-source, freeware, etc. must be approved by IT cell before using or downloading such software.

5.1.1a Purchase of software

The purchase of all software must adhere to this Policy.

The purchase of software should be from authorized partners or reputable software sellers.

All software purchases should be supported by standard support requirements, subscription period, and compatibility with the campus's server and hardware system.

The Registrar must authorize any changes from the above requirements.

5.1.1b Obtaining Software and renewal.

The university procures software and licenses from time to time. The perpetual license is for a lifetime. The renewal of the Academic license is carried out once a year or every 3 years.

5.1.1c Obtaining Open Source or Freeware Software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

IT cell approval is required if open source or freeware software is needed.

All open-source or freeware must be compatible with the campus's hardware and software systems.

6. Hardware Purchasing Policy

Policy Number: 6.1

Policy Date: 11-09-2020

Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners, etc.

Purpose of the Policy

This Policy provides guidelines for the campus purchase of hardware to ensure that all hardware technology for the campus is appropriate, value for money, and, where applicable, integrates with other technology for the campus. The objective of this Policy is to ensure that there is minimum diversity of hardware within the campus.

Procedures

6.1.1 Purchase of Hardware

The purchase of all desktops, servers, portable computers, computer peripherals, and devices must adhere to this Policy.

The procurement has to specify the budgetary source (ex. College/Research/TEQIP/ Govt etc.)

The procurement requestion form is duly signed by the head of the department and The Registrar

6.1.1a Purchasing Desktop and Laptop computer systems

The desktop computer systems purchased must run a relevant operating system here, e.g., Windows 8.1 and above, Linux versions, and integrate with the existing hardware to connect the campus servers.

The desktop computer systems must be purchased as standard desktop system bundle and must be such as HP, Dell, Lenovo, ASUS, etc.

The desktop computer system bundle must include:

Desktop tower

The desktop screen of {insert screen size here}

Keyboard and mouse You may like to consider stating if these are to be wireless

{insert name of the operating system, e.g., Windows 8.1, and software, e.g., Office 2013 here}

{insert other items here, such as speakers, microphone, webcam, printers, etc.}

The minimum capacity of the desktop must be:

- i3, 8th Generation of computer (GHz -gigahertz)here}
- 4GB memory (RAM) size
- 4 number of USB ports
- Optional: such as DVD drive, microphone port, etc.

The Registrar must authorize any change from the above requirements.

All desktops' purchases must be supported by 3/3/3 years warranty and be compatible with the campus's server system.

6.1.1b Purchasing Server Systems

A recommended IT specialist can only purchase server systems.

Server systems purchased must be compatible with all other computer hardware on the campus.

All purchases of server systems must be supported by 3/3/3 guarantee and warranty requirements.

The Registrar must authorize any change from the above requirements

The latest and existing hardware technology will be covered under AMC for better availability.

6.1.1c Purchasing computer peripherals

Computer system peripherals include add-on devices such as printers, scanners, external hard drives, etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software on the campus.

The department head can only authorize the purchase of computer peripherals.

The standard warranty must support all purchases of computer peripherals

7 IT Procurement Procedure

Policy Number: 1.1

Policy Date: 10-09-2020

At KLE Technological University, we acknowledge the importance of procurement of the right goods at the right cost. There are three sections for procurement viz—equipment, Softwares, and Consumables. The procurement is done through university funds, research grants, TEQIP grants, other Govt. grants, etc.

7.1.1 Purpose of the Procedure

This procedure provides guidelines to make the most of your budget, to procure quality goods and services in the right quantity at the lowest price possible, and at the right time, from the best vendor out there.

7.1.2 Procurement Procedure

- Upon receiving permission for procurement duly signed by head of the department and The Registrar. Letter has to be forwarded to the IT Cell.
- IT Cell will process the requestion based on the category.
- For Equipment and Software:
  i. The specification and details are verified.
  ii. The quotation request is sent to minimum of three authorised vendors and suppliers to quote with detailed specification.
  iii. The quotation is received in the sealed and closed envelope.
  iv. The procurement committee is formed and is consists of the department head for the department whose procurement is being carried-out, Coordinator IT Cell, The Registrar *(in special cases where the budget is high Finance Officer and two more heads or deans will be included in the committee)*.
  v. The sealed quotation is opened in the committee meeting.
  vi. The comparative statement is generated from the quotations received based on the specification, cost, warranty, payment terms and delivery.
  vii. The negotiation meeting will be conducted and purchase order is issued to the vendor.

8 Bring Your Own Device Policy

Policy Number: 8.1

Policy Date: 10-09-2020

At KLE Technological University, we acknowledge the importance of our own laptops and mobile technologies in improving campus communication and productivity. In addition to the increased use of own laptop and mobile devices, Staff and students have requested the option of connecting their laptop and mobile devices to KLE Technological University's network and equipment. We encourage you to read this document in full and to act upon the recommendations. This Policy should be read and carried out by all Staff and students.

8.1.1 Purpose of the Policy

This Policy provides guidelines for the use of personally owned notebooks, smartphones, tablets for campus purposes. All Staff and students who use or access KLE Technological University's technology equipment and/or services are bound by this Policy's conditions.

Each employee who utilizes personal mobile devices agrees:

- Not to download or transfer campus or personally sensitive information to the device. Sensitive information of campus or personal information that you consider sensitive to the campus, for example, intellectual property, other employee details, etc.
- To make every reasonable effort to ensure that KLE Technological University's information is not compromised through the use of laptop and mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorized persons and all registered devices should be password protected
- To maintain the device with licensed operating software, current antivirus security software, etc.
- Not to share the device with other individuals to protect the campus data access through the device.
- To abide by KLE Technological University's internet policy for appropriate use and access of internet sites etc.

- Not to connect USB memory sticks from an untrusted or unknown source to KLE Technological University's equipment.

9 E-wastage Policy

Policy Number: 9.1

Policy Date: 10-09-2020

At KLE Technological University, we acknowledge the importance of e-wastage. E-waste is generated as a result of any of the below-mentioned reasons:

Upgrade and innovation in technology.

Lifestyle changes.

End of the intended usage.

The write-off method is often used for IT goods considered non-repairable and obsolete to the university.

9.1.1 Purpose of the Policy

The e-waste management policy plays a crucial role in achieving sustainable e-waste management. This policy aims to ensure that effective procedures are implemented for the handling, storage, transportation, and disposal of e-waste generated from the activities on site.

9.1.2 Procedure of the Policy

Infocell will initiate the processes the e-waste at the campus. The priority is given to repair and reuse. Later if it is non-repairable and obsolete, then the new item is procured under buyback. Finally, the scraping of e-waste takes place if the above two clauses did not fit in.