JNTU

KAKINADA

Information Technology Policy and Procedure Manual

Jawaharlal Nehru Technological University Kakinada

Kakinada-533003, Andhra Pradesh, India.

Information Technology Policy and Procedure Manual

Table of Contents

Introduction

The **Jawaharlal Nehru Technological University Kakinada (JNTU Kakinada)** IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the University which must be followed by all staff. It also provides guidelines **JNTU Kakinada** will use to administer these policies, with the correct procedure to follow.

JNTU Kakinada 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, or to add new procedures.

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

These policies and procedures apply to all employees.

Technology Hardware Purchasing Policy

Policy Number: JNTUK/THPP1.0

Policy Date: 20-12-2022

/*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*/.

Purpose of the Policy

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

Procedures

Purchase of Hardware

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

Purchasing Desktop/Laptop Computer Systems

The desktop computer systems purchased must run a Suitable Operating System and integrate with required hardware. The desktop computer systems must be purchased as standard desktop system bundle.

The desktop computer system bundle must include:

- Operating system and any Software's (as per the requirement)
- Processor, Internal & External Memory
- Keyboard, mouse speakers, microphone, webcam etc.

Any requirements with a technical specification must be authorised by a technical team and approved by the Registrar, JNTU Kakinada. All purchases of desktops/laptops must be supported by guarantee and/or warranty requirements and OEM. All purchases for desktops/laptops must be in line with the JNTU Kakinada purchasing policy.

Purchasing Server Systems

Server systems purchased must be compatible with all other computer hardware in the University. All purchases of server systems must be supported by OEM, guarantee and/or warranty requirements and be compatible with the University's other server systems. Any change from the above requirements must be approved by the Registrar, JNTU Kakinada. All purchases for server systems must be in line with the JNTU Kakinada purchasing policy.

Purchasing Computer Peripherals

Computer system peripherals include 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 in the University.

All purchases of computer peripherals must be supported by guarantee and/or warranty requirements and be compatible with the University's other hardware and software systems. Any change from the above requirements must be authorised by the Registrar, JNTU Kakinada. All purchases for computer peripherals must be in line with the JNTU Kakinada purchasing policy.

Policy for Getting Software

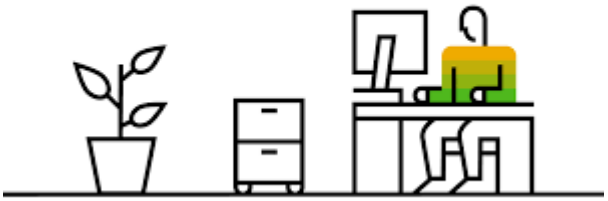
Policy Number: JNTUK/PGS1.0

Policy Date: 20-12-202

/*This policy should be read and carried out by all staff*/

Purpose of the Policy

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



Procedures

Request for Software

The proposal for purchase of a Software made by any department/unit is to be technically verified by the concerned department/ unit and further to be verified/authorised by Digital Monitoring Cell(DMC), JNTU Kakinada.

Purchase of Software

The purchase of all software must adhere to this policy.

All software technically authorised /recommended by Digital Monitoring Cell, JNTU Kakinada must be purchased from reputed software firms. All purchases of software must be supported by guarantee and/or warranty requirements and be compatible with the University's server and/or hardware system. Any changes from the above requirements must be authorised by the Registrar JNTU Kakinada. All purchases for software must be in line with the JNTU Kakinada purchasing policy.

Obtaining Open Source or Freeware Software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet. In the event that open source or freeware software is required, approval from Digital Monitoring Cell, JNTU Kakinada must be obtained prior to the download or use of such software. All open source or freeware must be compatible with the University's hardware and software systems. Any change from the above requirements must be authorised by the Registrar JNTU Kakinada.

Policy for Use of Software

Policy Number: JNTUK/PUS1.0

Policy Date: 20-12-2022

/* This policy should be read and carried out by all staff*/.

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the University to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

Software Licensing

All computer software copyrights and terms of all software licences will be followed by all employees/staff of the University. Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of Digital Monitoring Cell, JNTU Kakinada to ensure these terms are followed. Digital Monitoring Cell, JNTU Kakinada is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and licence agreements are adhered to.

Software Installation

All software must be appropriately registered with the supplier where this is a requirement. JNTU Kakinada 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 University's computers.

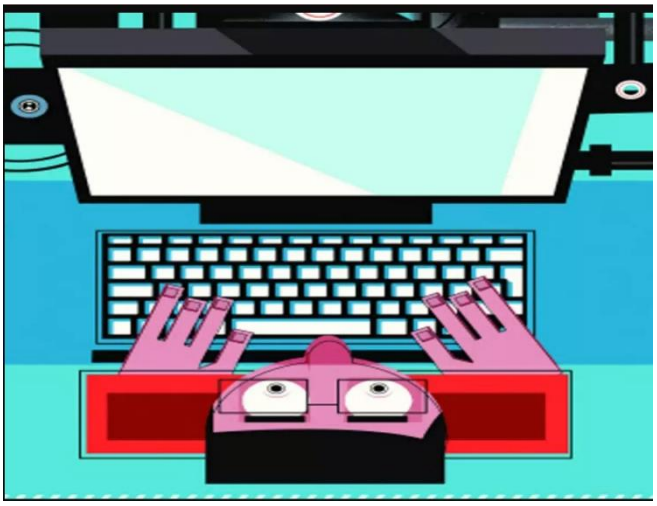
Digital Monitoring Cell, JNTU Kakinada carries out the software installation. A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

Software Usage

Only software purchased in accordance with the getting software policy is to be used within the University. Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software (on request/need based). This includes new employees to be trained to use existing software appropriately. This will be the responsibility of Digital Monitoring Cell, JNTU Kakinada. Employees are prohibited from bringing software from home and loading it onto the University's computer hardware.

Unless express approval from Digital Monitoring Cell, JNTU Kakinada is obtained, software cannot be taken home and loaded on an employees' home computer.

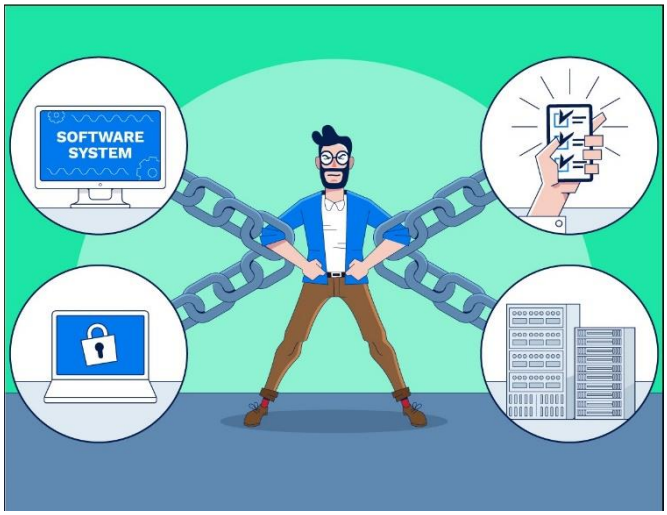


Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation from Digital Monitoring Cell, JNTU Kakinada is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the University and must be recorded on the software register by Digital Monitoring Cell, JNTU Kakinada. Unauthorised software is prohibited from being used in the University. This includes the use of software owned by an employee and used within the University.

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

Breach of Policy

Where there is a breach of this policy by an employee, that will be referred to the Registrar, JNTU Kakinada by the DMC for reprimand action. Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the Registrar, JNTU Kakinada immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then the DMC will refer the breach to the Registrar, JNTU Kakinada for further action.



Bring Your Own Device Policy

Policy Number: JNTUK/BODP1.0

Policy Date: 20-12-2022

At JNTU Kakinada we acknowledge the importance of mobile technologies in improving University communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to JNTU Kakinada'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.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and other types of mobile devices for University purposes. All staff who use or access JNTU Kakinada s technology equipment and/or services are bound by the conditions of this Policy.

Procedures

Current Mobile Devices Approved for University Use

The following personally owned mobile devices are approved to be used for University purposes:

- Mobile devices such as notebooks, smart phones, tablets, iPhone, removable media etc.

Registration of Personal Mobile Devices for University Use

/*You will need to consider if the University is to have any control over the applications that are used for University purposes and/or used on the personal devices*/.

Employees when using personal devices for University use will register the device with O/o the Registrar, JNTU Kakinada and this office will record the device and all applications used by the device.

Personal mobile devices can only be used for the following University purposes:

- Email access, University internet access, University telephone calls etc.

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer University or personal sensitive information to the device. Not to use the registered mobile device as the sole repository for JNTU Kakinada's information. All University information stored on mobile devices should be backed up

- To make every reasonable effort to ensure that JNTU Kakinada's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected

- To maintain the device suitable operating software and security software etc.
- Not to share the device with other individuals to protect the University data access through the device.
- To abide by JNTU Kakinada 's internet policy for appropriate use and access of internet sites etc.
- To notify JNTU Kakinada immediately in the event of loss or theft of the registered device.
- Not to connect USB memory sticks from an untrusted or unknown source to JNTU Kakinada's equipment.

All employees who have a registered personal mobile device for University use acknowledge that the University:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data
- Will regularly back-up data have held on the device
- Will delete all data held on the device in the event of loss or theft of the device
- Has first right to buy the device where the employee wants to sell the device
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
- Has the right to deregister the device for University use at any time.

Keeping Mobile Devices Secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

Exemptions

This policy is mandatory unless the Registrar JNTU Kakinada grants an exemption. Any requests for exemptions from any of these directives, should be referred to the JNTU Kakinada.

Breach of this Policy

DMC will report any breach of this policy to the Registrar JNTU Kakinada. Registrar will review the breach and determine adequate consequences.

Indemnity

JNTU Kakinada bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify JNTU Kakinada against any and all damages, costs and expenses suffered by JNTU Kakinada arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by JNTU Kakinada.

Information Technology Security Policy

Policy Number: JNTUK/ITSP1.0

Policy Date: 20-12-2022

/* This policy should be read and carried out by all staff*/.

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the University to ensure integrity, confidentiality and availability of data and assets.

Procedures

Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through relevant security measures. It will be the responsibility of Digital Monitoring Cell, JNTU Kakinada to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify the Registrar JNTU Kakinada immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad etc. will be the responsibility of the employee who has been issued with the laptop, notepads, iPads, mobile phones etc. Each employee is required to use locks, passwords, etc. and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, the Registrar JNTU Kakinada will assess the security measures undertaken to determine if the employee will be required to reimburse the University for the loss or damage.

All laptop, notepads, iPads etc. when kept at the office desk is to be secured by security measure here, such as keypad, lock etc. provided by O/o the Registrar JNTU Kakinada.

Information Security

All relevant data – either general such as sensitive, valuable, or critical University data is to be backed-up.

It is the responsibility of the Registrar JNTU Kakinada to ensure that data back-ups are conducted Monthly and the backed up data is kept in secured place.

All technology that has internet access must have anti-virus software installed. It is the responsibility of Digital Monitoring Cell, JNTU Kakinada to install all anti-virus software and ensure that this software remains up to date on all technology used by the University.

All information used within the University is to adhere to the privacy laws and the University's confidentiality requirements.

Technology Access

Every employee will be issued with a unique identification code to access the University technology and will be required to set a password for access every 06 months. Each password is to be combination of number of alpha and numeric etc. and is not to be shared with any employee within the University. Digital Monitoring Cell is responsible for the issuing of the identification code and initial password for all employees.

Where an employee forgets the password or is 'locked out', then the Registrar, JNTU Kakinada is authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

Information Technology Administration Policy

Policy Number: JNTUK/ITAP1.0

Policy Date: 20-12-2022

/* This policy should be read and carried out by all staff*/.

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the University.

Procedures

All software installed and the licence information must be registered with the Digital Monitoring Cell, JNTU Kakinada. It is the responsibility of the Digital Monitoring Cell, JNTU Kakinada to ensure that this registered is maintained. The register must record the following information:

- What software is installed on every machine
- What licence agreements are in place for each software package
- Renewal dates if applicable.

The Digital Monitoring Cell, JNTU Kakinada is responsible for the maintenance and management of all service agreements for the University technology. Any service requirements must first be approved by the Registrar, JNTU Kakinada.

The Digital Monitoring Cell, JNTU Kakinada is responsible for purchasing/ maintaining adequate technology spare parts and other requirements. A technology audit is to be conducted annually by the Digital Monitoring Cell, JNTU Kakinada to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to the Registrar, JNTU Kakinada.

Website Policy

Policy Number: JNTUK/WP1.0

Policy Date: 20-12-2022

Guidance: This policy should be read and carried out by all staff. Edit this policy so it suits the needs of your University.

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the University website.

Procedures

Website Register

The website register must record the following details:

- List of domain names registered to the University
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

The keeping the register up to date will be the responsibility of Web Development Cell, JNTU Kakinada. WDC will be responsible for any renewal of items listed in the register.

Website Content

All content on the University website is to be accurate, appropriate and current. This will be the responsibility of Web Development Cell, JNTU Kakinada

All content on the website must follow the University requirements. The content of the website is to be reviewed bi monthly.

Web Development Cell, JNTU Kakinada is authorised to make changes to the University website. Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the University. All data collected from the website is to adhere to the JNTU Kakinada Privacy Policy.

Electronic Transactions Policy

Policy Number: JNTUK/ETP1.0

Policy Date: 20-12-2022

/* This policy should be read and carried out by all staff

Purpose of the Policy

This policy provides guidelines for all electronic transactions undertaken on behalf of the University. The objective of this policy is to ensure that use of electronic funds transfers and receipts are started, carried out, and approved in a secure manner.

Procedures

Electronic Funds Transfer (EFT)

It is the policy of JNTU Kakinada that all payments and receipts should be made by EFT where appropriate.

The following Modules use EFT

1. Examination Fees
2. Affiliation Fees
3. Admission Fees

These payment modules use SBI epay/ SBI Collect Gateways and follow guidelines/procedures prescribed by the respective Gateways

IT Service Agreements Policy

Policy Number: JNTUK/ITSAP1.0

Policy Date: 22-12-2022

/* This policy should be read and carried out by all staff*/.

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the University.

Procedures

The following IT service agreements can be entered into on behalf of the University:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of University software
- Provision of mobile phones and relevant plans
- Website design, maintenance etc.

All IT service agreements must be reviewed by O/o the Registrar JNTU Kakinada before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by the Registrar JNTU Kakinada All IT service agreements, obligations and renewals must be recorded. Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorised by the Registrar JNTU Kakinada.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, O/o the Registrar JNTU Kakinada before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by the Registrar JNTU Kakinada.

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to the Registrar JNTU Kakinada who will be responsible for the settlement of such dispute.

Emergency Management of Information Technology Policy

Policy Number: JNTUK/EMIT1.0

Policy Date: 20-12-2022

/* This policy should be read and carried out by all staff*/.

Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the University.

Procedures

IT Hardware Failure

Where there is failure of any of the University's hardware, this must be referred to O/o the Registrar JNTU Kakinada immediately.

It is the responsibility of the Digital Monitoring Cell, JNTU Kakinada to take relevant actions in the event of IT hardware failure.

It is the responsibility of the Digital Monitoring Cell, JNTU Kakinada to undertake tests on planned emergency procedures regularly to ensure that all planned emergency procedures are appropriate and minimise disruption to University operations.

Virus or Other Security Breach

In the event that the University's information technology is compromised by software virus or any other malicious programmes such breaches are to be reported to the Digital Monitoring Cell, JNTU Kakinada immediately.

The Digital Monitoring Cell, JNTU Kakinada is responsible for ensuring that any security breach is dealt with within one day to minimise disruption to University operations.

Website Disruption

In the event that University website is disrupted, the following actions must be immediately undertaken by Web Development Cell (WDC), JNTU Kakinada.

- Website host to be notified
- The Registrar JNTU Kakinada must be notified immediately

o0o

JNTUK IT Policy