# Minutes of Meeting to Finalize Draft-IT Policy (2022)

**Date: 01/12/2023**
**Time: 11 AM Onwards**
**Venue: Head Cabin, DCSE, Brambe**

**Members:**

| Sr.No | Name |
|---|---|
| 1. | Prof. S. C Yadav, Prof, DCSE & Technical Cell (I/C), Chairman |
| 2. | Prof. Anurag Deep, Indian Law Institute, New Delhi, External Member |
| 3. | Prof. Ajai Singh, Head, Dept. of Civil Engineering, Member |
| 4. | Finance Officer/Nominee, Member |
| 5. | Dr. Nagapavan Chintalapati, Asst. Prof, DBA, Member |
| 6. | Dr. Vijay Kumar Yadav, Asst Prof, Dept. of Education, Member |
| 7. | Ltr. Cdr. Ujjawal Kumar (Redt), DR-II, Member |
| 8. | Dr. Kanojia Sindhuben Babulal, Asst. Prof, DCSE, Member |
| 9. | Dr. Pushpendra Kumar, Asst Prof, DCSE, Invitee Member |

The meeting commenced with a brief introduction and welcome from Prof. S.C Yadav (Chairman, IT Policy).

**Agenda:** Finalization of Draft IT – Policy 2022

**Resolution:** Prof. Yadav presented the final draft of the IT policy, highlighting key revisions and incorporating feedback received. All the members agreed on the final draft of IT Policy-2022. Chairman thanked all attendees for their valuable contributions throughout the drafting and review process.

Dr. Pushpendra Kumar | Dr. K. S Babulal | Dr. Vijay Kr Yadav

05/12/2024

Dr. Nagapavan Chintalapati | Ltr Cdr Ujjawal Kumar (Retd.), DR-II | FO/Nominee

Prof. Ajai Singh | Prof. Anurag Deep (online) | Prof. S. C Yadav 01/12/23

# Table of Contents

C150



CNUpavan

**Abbreviations** used in the document

C148

| Abbreviation | Full Form |
|---|---|
| IT | Information technology |
| IoT | Internet of Things |
| ICT | Information and Communications Technology |
| OSS | Open Source Software or freeware software |

# Central University of Jharkhand IT Policy

***"The NEP 2020 aims at promoting online education consequent to the recent rise in epidemics and pandemics to ensure preparedness with alternative modes of quality education whenever and wherever traditional and in-person modes of education are not possible, has been covered. A dedicated unit to orchestrate the building of digital infrastructure, digital content and capacity building will be created in MHRD to look after the e-education needs of both school and higher education."***

**Preamble**

The CUJ IT Policy aims to promote and regulate digital infrastructure, digital content and online activities within the University with an emphasis on safe and responsible use of information and communication technology. In the light of National Education Policy (NEP) and following recent epidemic situations, the policy document addresses e-education needs and ensures preparedness for implementation of hybrid mode of learning.

## 1. Introduction

Central University of Jharkhand is also proposing to have its own IT Policy that works as guidelines for using the university's IT Infrastructure including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called "Information Technology (IT)". Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this university.

Use of Central University of Jharkhand's network and computer resources should support the basic missions of the University in teaching, learning and research. Users of Central University of Jharkhand's network and computer resources ("users") are responsible to properly use and protect information resources and to respect the rights of others. This policy provides guidelines for the appropriate use of IT resources.

**IT policies and related standards apply to all users across the entire Central University of Jharkhand and on campus visitors. This policy apply whether the university's information resources are accessed on- or off-campus**.

This policy covers the appropriate use of all IT resources including hardware, software, systems, networks, procurement and maintenance, information security and the information contained therein.

The purpose of this policy is to define rules and requirements for connecting to CUJ's networks and systems from any host. These rules and requirements are designed to minimize the potential exposure to students, faculty, employees, vendors, contractors, guests and other affiliates of CUJ as well as to the CUJ itself from damages, which may result from unauthorized use of CUJ resources. Potential damages include but are not limited to the loss of sensitive or confidential data or intellectual property, damage in public image, damage to critical CUJ

internal systems, and fines or other financial liabilities that could be incurred because of those losses. Also, it provides a security framework that will ensure the protection of University Information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. University Information may be verbal, digital, and/or hardcopy, individually-controlled or shared, stand-alone or networked, used for administration, research, teaching, or other purposes.

Further, due to the dynamic nature of Information Technology, Information security in general and therefore policies that govern information security processes are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

The policy applies to all the members of the University and others who handle University managed information including faculty, staff, student, contractors, consultants and visitors of the University. The University abide “The Digital Personal Data Protection Act, 2023.

**1.1 Purpose and Scope of IT Policy:**

1.1.1 CUJ Provide IT resources to its end-user to enhance their efficiency and productivity. These resources are meant as tools to access and process information related to their areas of work. These resources help officials to remain well informed and carry out their functions in an efficient and effective manner.

1.1.2. For the purpose of this policy, the term ‘IT Resources’ includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

1.1.3. Misuse of these resources can result in unwanted risk and liabilities for the CUJ. It is, therefore, expected that these resources are used primarily for CUJ related purposes and in a lawful and ethical way.

**1.2 Scope:**

1.2.1. This policy governs the usage of IT resources from an end user perspective.
1.2.2. This policy is applicable to all the end users of CUJ.

**1.3 Objective:**

1.3.1. The objective of this policy is to ensure proper access to and usage of IT infrastructure and assets of CUJ and prevent their misuse by the users. Use of resources provided by the Government of India implies the user's agreement to be governed by this policy.

### 1.4 Access to the Network (Internet and Intranet):

a. A user should register the client system and obtain one time approval /permission from the Technical Cell before connecting the client system to the CUJ network.

b. Users should not undertake any activity through any website or applications to bypass filtering / Policy / Firewall / UTM of the network or perform any other unlawful acts which may affect the network's performance or security

c. Users are not allowed to change the NIC configuration, IP address or any other parameters set for accessing University's LAN & WAN without permission of the Technical Cell.

d. Users shall not connect any other devices to access Internet / any other network in the same client system configured for connecting to LAN/WAN of the University without permission.

e. It is the responsibility of the user to ensure that the client system is free from any Virus/Malware/Potential threat softwares/pirated copy of softwares before connecting to the University's network.

### 1.5 Access to the CUJ Wireless network:

For connecting to a CUJ wireless network, user should ensure the following:

a. A user should register the access device and obtain one time approval / permission from the Technical Cell before connecting the access device to the CUJ wireless network.

b. Wireless client systems and wireless devices should not be allowed to connect to the CUJ wireless access points without due authentication.

c. To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

### 1.6 Filtering and blocking of Sites:

a. Technical Cell may block content over the Internet which is in contravention of the relevant provisions of the Government Laws and other applicable laws or which may pose a security threat to the network.

b. Technical Cell may also block content, which, in the opinion of the University, is inappropriate or may adversely affect the network security and productivity of the users/organization.

### 1.7 Approving Authority:

1. Executive Council
2. Finance Committee
3. Vice Chancellor
4. Technical Cell

### 1.8 Applicability:

Applies to all University students, faculty and staff, and all others using computer and communication technologies, including the University's network, whether personally or University owned, which access, transmit or store University or student information. This policy also applies to all other individuals and entities granted use of University Information, including, but not limited to, contractors, temporary employees, and others as identified by university.

Stakeholders on campus or off campus

- ✓ Students: UG, PG, Research
- ✓ Employees (Permanent/ Temporary/ Contractual)
- ✓ Faculty (Permanent/Temporary/Contractual)
- ✓ Administrative Staff (Non-Technical / Technical)
- ✓ Higher Authorities and Officers
- ✓ Guests

## 1.9 Resources

- Network Devices wired/ wireless
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Desktop / Laptop server computing facility
- Software
- Documentation facility (Printers/Scanners)
- Multimedia Contents

# 2. Installation Policy

## 2.1 IT Hardware Installation

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

**A. Who is the Primary User?**

· Computer System issued individual (Administrative officers/Faculty/staff/research scholar), that individual will be responsible for that system.

· Those systems in the lab/office, department Head should make an arrangement and make a person (lab coordinator) responsible for compliance.

**B. What are End User Computer Systems?**

· Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the TECHNICAL CELL, are still considered under this policy as "end-users" computers.

**C. Warranty and Annual Maintenance Contract**

· Any IT equipment purchased by the University and provided to primary users will be maintained under annual maintenance contract.

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract .

· The above said maintenance will be under the supervision of the Technical Cell.

**D. Power Connection to Computers and Peripherals**

· All the computers and peripherals should be connected to the electrical point strictly through UPS. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

· All the power connection related issues/ installation of ups/earthing/wiring related issues will be dealt with by the Engineering Section of CUJ.

**E. Shifting Computer from One Location to another**

· Computer systems may be moved from one location to another with prior written intimation to the TECHNICAL CELL, as TECHNICAL CELL maintains the record of computer identification names and MAC address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation (from the list maintained by TECHNICAL CELL is found for any computer system, network connection would be disabled and the same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs the Technical Cell in writing/by email, connection will be restored.

**F. Noncompliance**

· CUJ faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computers resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even the whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be non-compliant.

## 2.2 Software Installation and Licensing

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 anti-piracy laws, University IT policy does not allow any unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, the university will hold the department/individual personally responsible for any unauthorized software installed on the computers located in their department/individual's rooms.

### A. Operating System and its Updating

**1.** Individual users should make sure that respective computer systems have their OS updated of their service packs/patches, through the Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

**2.** University as a policy encourages the user community to go for open source software such as Linux, Open office etc..to be used on their systems wherever possible.

### B. Antivirus Software and its updating

**1.** Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system safe from Virus, Malware, Trojan etc.

**2.** 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.

**3.** If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from Technical Cell or any service-providing agency.

**4.** Do not remove or disable anti-virus software.

**5.** Do not use unauthorized/ not licensing Antivirus Solution.

**6**. Centralized or network based antivirus shall be installed.

### C. Backups of Data

**1.** Individual users are responsible to perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible and the loss of data is the sole responsibility of the individual.

**2.** Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned in at least two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only C drive volume will protect the data loss. However, it is not a foolproof solution. Apart from this, users should keep their valuable data either on portable hard disks or other reliable storage devices.

## 2.3 Network Device Connectivity and Installation:

Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection, a Virtual Private Network (VPN) connection, or Wireless Connection is governed under the University IT Policy.

### IP Address Allocation:

- ✓ Any computer (PC/laptop/Server) that will be connected to the university network should have an IP address assigned by the TECHNICAL CELL. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.
- ✓ Any IP base device like network printer, smart TV, biometric machine, CCTV DVR, IP Camera, Video conferencing device, IP Phone etc. is to be installed at any location, then the concern user should contact TECHNICAL CELL and get proper IP Address.
- ✓ Any computer (PC/Server) that will be connected to the university network should have an IP address assigned by the TECHNICAL CELL.
- ✓ All network devices should be IPV6 compliant and should support IPV4 till the time all networks and applications are not completely migrated to IPV6.
- ✓ Following a systematic approach, the range of IP addresses that will be allocated to each department/section/hostel etc. is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool.

### A. Wireless Local Area Networks:

- ✓ This policy applies, in its entirety, to School, department, or division wireless local area networks. In addition to the requirements of this policy, schools, departments, or divisions must register each wireless access point with TECHNICAL CELL including Point of Contact information. TECHNICAL CELL Will be responsible for creating wireless access points.

- ✓ School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.
- ✓ If individual departments/schools etc.. wants to have an inter-building wireless network, prior to installation of such network, it should obtain permission from the University authorities.

### B. Structured Cabling as a part of New Buildings:

- ✓ All the new buildings that will be constructed in the academic complex here onwards should have the structured cabling included in their building plans like any other wiring such as electrical and telephone cabling, for LAN as a part of the building layout Plan.
- ✓ Engineering Cell/Section may make provisions in their designs for network points/access points in each room and in the corridors based on the input provided by TECHNICAL CELL or in coordination with TECHNICAL CELL. All such network cabling should strictly adhere to the structured cabling standards used for Local Area Networks.

# 3. Email Policy:

## 3.1 E-mail, password and security Policy:

3.1.1 The University uses email as a major mode of communication. Communications include university data that travels as part of mail transactions between users located both within the university and outside.

3.1.2 This policy of Central University of Jharkhand lays down the guidelines with respect to use of CUJ e-mail services. The Implementing Department of University E-mail Service shall be the Technical Cell, CUJ.

3.1.3 This policy is based on the E-mail Policy adopted by the Govt. of India, with suitable changes.

## 3.2 Scope:

3.2.1 Only the e-mail services provided by G-Suite (www.cuj.ac.in), of Google shall be used for official communications by the university. Every staff, faculty member, and research student shall be mandatorily required to use the official email id allotted to them in conducting their communications relating to the University. E-mail services provided by other service providers shall not be used for any official communication.

3.2.2 This policy is applicable to all primary user/ end-user / research students of

CUJ that use these e-mail services and choose to adopt this policy in future. The directives contained in this policy must be followed by all of them with no exceptions.

3.2.3 E-mail can be used as part of the electronic file processing in university.

## 3.3 Objective:

3.3.1 The objective of this policy is to ensure secure access and usage of university e-mail services by its users. Users have the responsibility to use this resource in an efficient, effective, lawful, and ethical manner. Use of the CUJ e-mail service amounts to the user's agreement to be governed by this policy.

3.3.2 All services under e-mail are offered free of cost to all officials under Departments/ Centres and research students enrolled in the University.

3.3.3 Any other policies, guidelines or instructions on e-mail previously issued shall be superseded by this policy.

## 3.4 Basic requirements of CUJ email Service:

### 3.5.1 Security

a) Considering the security concerns with regard to a sensitive deployment like e-mail, apart from the service provided by the Technical Cell, there would not be any other email service under the university.

b) Secure access to the university email service

(1) It is recommended for users working in sensitive offices to use 2-Step Verification (also known as two-factor authentication)/OTP for secure authentication as deemed appropriate by the competent authority.

(2) It is recommended that university officials on long deputation/ stationed abroad and handling sensitive information should use 2-Step Verification (also known as two-factor authentication)/ OTP for accessing university email services as deemed appropriate by the competent authority.

c) From the perspective of security, the following shall be adhered to by all users of university e-mail service:

(1) Users shall not download emails from their official email account, configured on the university mail server, by configuring POP or IMAP on any other email service provider. This implies that users should not provide their university e-mail account details (id and password) to their accounts on private email service providers.

(2) In case a compromise of an e-mail id is detected by the Technical Cell, an SMS alert shall be sent to the user on the registered mobile number. In case an “attempt” to compromise the password of an account is detected,

an e-mail alert shall be sent. Both the e-mail and the SMS shall contain details of the action to be taken by the user. In case a user does not take the required action even after five such alerts (indicating a compromise),the Technical Cell reserves the right to reset the password of that particular email id under intimation to the Registrar/Vice Chancellor/concerned designated officer of the respective Department/Centre.

(3) In case of a situation when a compromise of a user id impacts a large user base or the data security of the deployment, the Technical Cell shall reset the password of that user id. This action shall be taken on an immediate basis, and the information shall be provided to the user, the competent authority and the concerned designated officer of the Department/Centre subsequently. SMS shall be one of the prime channels to contact a user; hence all users should ensure that their mobile numbers are updated.

(4) Auto-save of password in the Government email service shall not be permitted due to security reasons.

### 3.5.2 Email Account Management

a) Based on the request of the respective department/Centre, Technical Cell will create two ids, one based on the designation and the other based on the name. Designation based ids are recommended for officers dealing with the public. Use of alphanumeric characters as part of the e-mail id is recommended for sensitive users as deemed appropriate by the competent authority.

b) University officers who quit, resign or superannuate shall be allowed to retain the name-based e-mail address i.e.userid@cuj.ac.in for two-year post resignation or superannuation upon approval from the competent authority. The personal details of His/her email account shall be updated and his account shall be delisted from all the concerned group emails immediately upon leaving the University.

### 3.5.3 Delegated Admin Console

Delegated Admin Console can only be handled by Technical Cell. For security reasons, no other department/center/section/unit may be allowed to access the Administrator Account. Only Technical Cell is authorized to create/ delete/ change the password of user ids under that respective domain as and when required.

### 3.5.4 E-mail Domain

By default, the address "userid@cuj.ac.in" shall be assigned to the users. The user id shall be created as per the addressing policy mentioned in email creation form.

### 3.5.5 Use of Secure Passwords

All users accessing the e-mail services must use strong passwords for security of their email accounts.

### 3.5.6 Privacy

Users should ensure that emails are kept confidential. Technical Cell shall take all possible precautions on maintaining privacy. Users must ensure that information regarding their password or any other personal information is not shared with anyone. However, it must be kept in mind that emails are not fully secure and care should be taken when typing email addresses to ensure that it reaches the intended recipient. Moreover, it is also possible that the origin of an email is not what it appears to be and users should not disclose sensitive information such as passwords/any financial information in emails.

## 3.6 Responsibilities of Department/Cell/Section:

### 3.6.1 Policy Compliance

a) All Department/Cell/Section shall implement appropriate controls to ensure compliance with the e-mail policy by their users. Technical Cell shall give the requisite support in this regard.

b) The Department/Cell/Section shall ensure that official email accounts of all its users are created only on the e-mail server of the university**.**

c) Head of Department (HoD) of the department/cell/ section/ unit shall ensure resolution of all incidents related to the security aspects of the e-mail policy. Technical Cell shall give the requisite support in this regard.

d) HoD shall ensure that training and awareness programs on e-mail security are organized at regular intervals. The Technical Cell shall provide the required support.

### 3.6.2 Policy Dissemination

a) Head of Department (HoD) of the concerned Department/Cell/Section should ensure dissemination of the e-mail policy.

b) Orientation programs for new teaching, non teaching staff, researchers etc shall include a session on the e-mail policy.

## 3.7 Responsibilities of Users:

### 3.7.1 Appropriate Use of E-mail Service

a) E-mail is provided as a professional resource to assist users in fulfilling their official duties. Designation based ids should be used for official communication and name-based ids can be used for both official and personal communication.

b) For personal communication, reasonable use of the email service is permitted provided it is not:

i. Of commercial/profit-making nature or used for personal financial gains.

ii. In conflict with University rules, regulations, policies, and procedures; including the email policy.

iii. In conflict with the end-user obligations towards the University as employer.

c) Bulk emails (including reply-all to such bulk emails) with multiple intended recipients (viz., faculty/ staff/ students) shall be routed through/ upon approval from, the office of the Registrar or the concerned head/ chairperson of the department/cell/section unit or committee.

d) Examples of inappropriate use of the email service

i. Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information, including email IDs and/or passwords.

ii. Unauthorized access of the services. This includes the distribution of emails anonymously, use of other officers' user ids or using a false identity.

iii. Creation and exchange of advertisements, solicitations and other unofficial, unsolicited e-mail (such as spam, chain emails).

iv. Creation and exchange of information in violation of any laws.

v. Willful transmission of an e-mail containing a computer virus.

vi. Misrepresentation of the identity of the sender of an email.

vii. Use or attempt to use the accounts of others without their permission.

viii. Transmission of emails involving language derogatory to religion, caste, ethnicity, sending personal emails to a broadcast list.

ix. Use of distribution lists for the purpose of sending emails that are personal in nature, such as personal functions, etc.

Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation of the account after consultation with the Competent Authority. Further, such instances may also invite scrutiny by the investigating agencies depending on the nature of violation.

### 3.7.2 User's Role

a) The User is responsible for any data/e-mail that is transmitted using the university e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.

b) Sharing of passwords is prohibited.

c) The user's responsibility shall extend to the following:

i) Users shall be responsible for the activities carried out on their client systems,

using the accounts assigned to them.

ii) The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.

iii) Back up of important files shall be taken by the user at regular intervals. The Technical Cell shall not restore the data lost due to the user's actions.

iv) Users should not open attachments in emails received from unsolicited/untrusted sources unless the attachment has been scanned for viruses.

d) The University may define and implement storage quotas for both end-user as well as student email accounts. Users are responsible for regular deletion of email which is not of use in order to save storage space. Users will be notified via email when they are approaching the end of their storage limit. Once the storage limit is exhausted, one final email will be sent to the user, notifying them to reduce the storage below the sanctioned limit. After exhaustion of the storage limit, users will not receive any further emails until the storage is reduced below the storage limit.

## 3.8 Scrutiny of emails/Release of logs:

**3.8.1** Logs comprise the flow of emails but not the content of the emails. Notwithstanding anything in the clauses above, the disclosure of logs/emails to law enforcement agencies and other departments/centers by the Technical Cell would be done only as per the IT Act, 2000 and other applicable laws.

**3.8.2** The Technical Cell shall neither accept nor act on the request from any other department/cell/section, save as provided in this clause, for scrutiny of e-mails or release of logs.

**3.8.3** The ownership of emails created or distributed using the University's email service vests with the University. Under usual circumstances, the University will respect the privacy of the email content. However, there may be exceptional situations/reasonable circumstances where the University may access emails(including their content) without prior notice and at any time, without the user's consent. Such access will require prior approval of the competent authority and the Head of the respective Department/Cell/Section responsible for the end-user /student. The exceptional situations/reasonable circumstances may include, but will not be limited to:

(i) Compliance with legal obligations/requirements.

(ii) Managing the email account after an end-user leaves the University, is terminated from their service.

## 3.9 Security Incident Management Process:

**3.9.1** A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of university data. Security incidents can be due to factors like malware, phishing, loss of a device, compromise of an e-mail id etc.

**3.9.2** It shall be within the right of the Technical Cell to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service.

**3.9.3** Any security incident, noticed or identified by a user, must immediately be brought to the notice of the Indian Computer Emergency Response Team(ICERT) and the Technical Cell

### 3.10 Deactivation:

3.11.1 In case of threat to the security of the University service, the e-mail id being used to impact the service may be suspended or deactivated immediately by the Technical Cell.

3.10.2 Subsequent to deactivation, the concerned user and the competent authority of that respective Department/Cell/Section shall be informed.

### 3.12 Exemption:

Departments/centers operating Intranet mail servers with air-gap are exempted from this policy.

### 3.13 Audit of E-mail Services:

The security audit of G-Suite email services and other departments maintaining their own mail server shall be conducted periodically by an outsourced agency as approved by the Technical Cell.

### 3.14 E-mail account and resultant record:

All the E-mail ids provided to the individual members of academic and administrative community, including the E-mail ids provided to different Branches, Sections, Divisions and Research Centres are supposed to transact the official business through these email ids.

### 3.15 Review:

Future changes in this Policy, as deemed necessary, shall be made by Technical Cell with the recommendation of IT Committee and approval of the competent authority .The above laid

down policies particularly 1 to 12 are broadly applicable even to the email services that are provided by other sources such as gmail.com, rediffmail.com, Hotmail.com, Yahoo.com etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

# 4. Network/Server Usage Policy and Guideline:

## 4.1 Individual/Stakeholders Responsibility

**Individuals must not:**

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which (CUJ) considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to (CUJ), alter any information about it, or express any opinion about (CUJ), unless they are specifically authorized to do this.

- Send unprotected sensitive or confidential information externally.
- Make official commitments through the internet or email on behalf of (CUJ) unless authorized to do so.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Care must be taken to not leave confidential material on printers or photocopiers. · Violate the IT ACT of GOI provided from time to time.

## 4.2 Guidelines for Desktop/PC/Laptop etc Users:

The Guidelines are meant for all members of CUJ Network User Community and users of University Network. Due to the increase in hacker activity, University IT Policy has put together recommendations to strengthen system security.

The following recommendations include:

i. All desktop computers should have the latest version of antivirus.

ii. When a desktop computer is installed, all operating system updates should be applied.

iii. All Windows desktops should have an administrator account that is not used as the regular login account.

iv. The password should be difficult to break. Suggested to mix upper case, lower case, or other characters not easily found in a dictionary, and make sure they are at least eight characters long. Also suggested to change the password on regular interval time.

v. Don’t open email or attachments from unknown sources.

vi. The guest account should be disabled.

vii. Disconnect from the Internet when not in use.

viii. When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.

ix. TECHNICALCELL recommends a regular backup strategy. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine. Departments should arrange/purchase data storage devices as part of the requirement from the department. If the user feels he/she can store data on Cloud etc.

x. Do not allow anyone else to use their user ID and password on any (CUJ) IT system

xi. Do not leave their user accounts logged in at an unattended and unlocked computer.

xii. Use someone else’s user ID and password to access (CUJ’s) IT systems. Do not leave the password unprotected (for example writing it down).

xiii. Documents that are no longer required to be shared will be removed from the shared folder.

xiv. All shared folders should be password protected.

xv. Remote Login should be disabled and only in special cases it would be permitted with permission of TECHNICAL CELL (Incharge).

xvi. End user will be solely responsible for use/installation of any unauthorized/restricted software.

## 4.3 Data Backup, Security, and Disclaimer

TECHNICAL CELL will not be liable for the loss or corruption of data on the individual user’s computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an TECHNICAL CELL staff member in the process of helping the user in resolving their network/computer related problems.

Users may note that the University’s Network Security System may maintain a history of infractions, for each user account. In case of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate University authorities.

## 4.4 Wi-Fi implementation and usage

### 4.4.1. Wi-Fi Access and locations

1. Wi-Fi Access Point: Wi-Fi facilities may be made available at canteen, library, hostels, department/cell/section, laboratories, guest house and officers residences etc. The decision of TECHNICAL CELL will be final to decide the location of such access points.

2. Wi-Fi Access Points: may be placed temporarily on demand in auditorium and other places, for conference, workshops, symposia and any other important events.
3. In special cases the individual or department may approach the technical cell to get proper secure configuration and registration of the personal/ department's Access Points or routers with proper approval of the concerned head.

### 4.4.2. Methods for Wi-Fi users Authentication/ Authorization and Activity Logs

1. For respected guests/invitees staying in the campus Wi-Fi access is given on demand by the corresponding hosts. It is password based access. Passwords are changed periodically by Technical Cell.
2. For others, some Wi-Fi can be accessible to all in specific areas like libraries etc with a per day limit on data on it.
3. Specific Wi-Fi installed in the department, if the Head of Department wants can give username password on request.

#### 4.4.3. Wi-Fi Usage

1. The individual user will be responsible for his/her Wi-Fi usage.
2. Solicited and ethical usage is expected from the users.
3. The Internet Access through Wi-Fi is filtered access. Possible phishing, spurious, unsolicited or obscene sites, gaming sites, some shopping/multimedia streaming sites are blocked at firewall level.
4. There shall be a per day usage quota on Students User class.
5. The users will access the University Resources properly and will not try to harm the resources.

#### 4.4.4. Misuse and actions

a. If a user or his/her device is causing any harm to university resources or other users, then such a user will be warned by THE CONCERNED DEPARTMENT OR TECHNICAL CELL. User's intention and device will be verified and the corresponding Head of the department will be informed accordingly.

b. A virus infected device may create noticeable network traffic or attempt cyber attacks. Then the user will be notified and his/her access shall be blocked until the infected device is cleaned/ free from viral infection.

## 4.5 Internet Access:

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. Network IDs will only be established for students, staff and faculty who are currently affiliated with the University. Students, staff and faculty who leave the University will have their Net Access ID and associated files deleted. No User will be allowed more than one Net Access

ID at a time, with the exception that faculty or officers, who hold more than one portfolio, are entitled to have Net Access ID related to the functions of that portfolio.

In special cases like workshop/seminar/conferences etc. access could be permitted by prior permission of competent authority.

**Limitations on the use of Resources/Data:** On behalf of the University, TECHNICAL CELL reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

The data downloaded/live stream like (movie/video/songs/gaming/software etc) is not allowed.

**Ethics and Etiquette**: The User will not attempt to override or break the security of the University networks, or machines accessible there from. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages.

## 4.6 Video Surveillance/CCTV Monitoring:

### A. The system

- ✓ The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.
- ✓ Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.
- ✓ Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.
- ✓ Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

### B. Purpose of the system

- ✓ The system has been installed by the university with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:
    - Deter those having criminal intent
    - Assist in the prevention and detection of crime
    - Facilitate the identification, apprehension and prosecution of offenders in

relation to crime and public order

### C. The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

### D. The Security Control Room

✓ Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

✓ No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers. Any other authorized member requiring access in special circumstances needs to get written permission from Vice chancellor and Registrar.

✓ Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Registrar and vice chancellor.

✓ Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization they represent, the person who granted authorization and the times of entry to and exit from the center. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

### E. Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

### F. Recording

✓ Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

✓ Images will normally be retained for **fifteen** days from the date of recording, and then automatically overwritten and the Log updated accordingly. Once a hard drive has

reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

✓ All hard drives and recorders shall remain the property of the university until disposal and destruction.

# 5. Web Site Hosting Policy

**5.1 For Official Pages:** Sections and departments may have pages on CUJ's official Web page. Official Web pages must conform to the University Web Site Creation Guidelines for Web site hosting.

**5.2 For Personal Pages:** Apart from Official profile on website, Faculty may request to have their personal pages linked to official web site of the university by sending a written request to Technical Cell giving the details of the hyperlink of the URL that he/she wants to be added in the official website of the university. However, his/her pages must be used for the purpose of academics and should not violate any university, state, or central government laws. Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the university.

## 5.3 Supply of Information by Section, Department for Publishing on /updating the CUJ Web Site:

Any Schools or Departments having any updated information should send a Hard Copy of such information duly signed by the competent authority/Heads of Section, Department, or Division level, along with a softcopy to be sent to the TECHNICAL CELL.

This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Section, Department, or Division. Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the webmaster upon receiving the written requests.

If such web pages have to be directly added into the official web site of the university, necessary content pages have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format.

Further, such requests along with the soft copy of the contents should be forwarded to the competent authority, TECHNICAL CELL well in advance (3 days).

## 5.4 General Information Technology Usage Guideline:

### a) Prohibited Use

Users must not send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of

applicable law or University policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.

**b) Copyrights and Licenses**

Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the University's information resources is a violation of this policy.

**c) Social Media**

Users must respect the purpose of and abide by the terms of use of online media forums, including social networking websites, mailing lists, chat rooms and blogs.

**d) Political Use**

University information resources must not be used for partisan political activities prohibited by central, state or other applicable laws, and may be used for other political activities only when in compliance with central, state and other laws and in compliance with applicable University policies.

**e) Personal Use**

University information resources should not be used for activities unrelated to appropriate University functions, except in a purely incidental manner.

**f) Commercial Use**

University information resources should not be used for commercial purposes, including advertisements, solicitations, promotions or other commercial messages. Any such permitted commercial use should be properly related to University activities, take into account proper cost allocations for government and other overhead determinations, and provide for appropriate reimbursement to the University for taxes and other costs the University may incur by reason of the commercial use.

**g) Risks:**

The University shall emphasize on managing the risks involved for the usage of IT resources. This shall include standard procedures for identification, minimization and monitoring of risk impact by preventive and corrective measures. This should also include procedures for timely data backup, replication and restoring policies, power backups, audit policies, alternate internet connectivity for a fail-safe internet access.

**h) Open Source Asset:**

The University shall endeavor towards the promotion and effective usage of open source software.

**i) Password Policy:**

Passwords are a critical element in maintaining the security of IT assets. All client machines should have a power-on password and login password. Remember password features should not be used.

**j) Safeguard your Equipment**: Adopt Security measures that protect your equipment against theft, fire and explosives.

**k) Protect your Power Supply**: Protect your equipment from power failures and electrical anomalies. Make sure that your power supplies will be provided without interruption and comply with the specifications provided by equipment manufacturers. Also consider multiple power feeds.

**l) Secure your Cables**: Protect your power lines and telecommunication cables from damage. Place power lines and telecommunication cables underground whenever those lines are connected to information processing facilities. Use Conduits to prevent unauthorized interception or damage to cables and lines.

**m) Maintain your Equipment**: Maintain your equipment to ensure that it functions properly. Follow the equipment manufacturers recommended maintenance specifications. Allow only authorized maintenance people to service your equipment and suggest keeping a record of all preventive and corrective maintenance activities.

# 6. Purchase/ Procurement Policy

## Summary

The policy is to establish the procedure for the purchase of computer hardware, software, networking equipment and allied material.

## 6.1 Procedure:

The purchase of computer hardware, software, networking equipment and allied material shall be done after the approval from the Central and Departmental Purchase committee. A member nominated by Technical Cell (Incharge) will be part of CPC/DPC for this purpose.

The technical cell will check the minimum configuration and warranty of the above said and may suggest accordingly.

The purchase procedure shall be as per the university rule.

**6.2 Warranty:** Procurement of IT Assets should cater for onsite warranty, as far as practicable for extended period. The warranty should cover all items of non-consumable nature including batteries of UPS, laptops and such other portable IT devices. The scope of warranty of Software should also include patches, updates/upgrades and associated changes of application and provision of help desk facility for providing support in structured and time bound manner.

## 6.3 Condemnation and Disposal of IT equipment:

The present disposal and condemnation policy follow the Guidelines vide circular No. 8-11/2012-13/IT-I dated 26/12/2014 of Department of Telecommunications, Ministry of

Communications & IT, Government of India and Notification No. F.No.29-6/2018-S&S dated 25/11.2022 issued by Ministry of Education, Department of Education, and Government of India

### 6.3.1 Applicability

These guidelines will be applicable to all IT equipment installed in CUJ.

**Note:**

i) Consumable items related to IT like used printer cartridges etc. are not included in the scope of scrapping on account of the fact of its nature as consumable.

ii) IT items like pen drives/floppies, which are petty valued and are not capitalized, are not qualified for the detailed scrapping procedure.

### 6.3.2 Grounds for Condemnation:

The IT equipment can be condemned on following grounds:

a) Equipment outlived its prescribed life and was certified by the IT Committee as unfit for its useful contribution. The prescribed life of various IT equipment in general would be 10 years. [IT IS SAID THAT NEW TECHNOLOGY IS COMING AFTER EVERY 18 MONTHS, DESKTOPS MAY BE REQUIRED TO BE REPLACED AFTER 6 YEARS AND LAPTOPS AFTER 3 YEARS] Software does not require any Physical Scrapping. The prescribed life of Battery of UPS would be 2 years after the warranty period.

b) Equipment which has become obsolete technology-wise and can't be upgraded and support from vendors, either paid or unpaid, does not exist and their use may result in insecurity threat/ unauthorized access to data.

c) Beyond economical repair: When repair cost is considered too high (exceeding 50% of residual value equipment taking depreciation into account), and the age of the equipment. Such cases should be dealt on a case-to-case basis and should have concurrence of finance. In case of IT equipment depreciation of 20% per year may be taken for calculation of residual value.

d) Equipment that has been damaged due to fire or any other unforeseen reason and have been certified as beyond repair by the authorized service agency and agreed upon by the IT.

### 6.3.3. Disposal:

A. Such equipment shall be disposed strictly following the procedure as laid down in Rule196 to 201 of GFR 2005 [General Financial Rules of Government of India available here https://doe.gov.in/order-circular/general-financial-rules-2005 ] and notification regarding disposal of E-Waste issued by Ministry of Environment, Forests, and Climate Change [available here https://cpcb.nic.in/e-waste/]. Once the equipment has been condemned, it should be removed from office use and

kept in the area allocated for scrapped equipment. University will also ensure removal of service and inventory labels from such equipment. AMC, if any, for such equipment/instruments shall be stopped with the effective date of scrapping. Essential data, if any, must be removed after taking proper backup and preserved by the user of the equipment.

B. The IT cell shall propagate the information [in the form of notice, demonstration, relevant videos etc.] on disposal of E-waste to all users [regarding their personal E-waste] through various departments once in a year as a part of an awareness programme.

**6.3.4. Procedure:**

a) Scrapping proposals will be initiated by the user section/IT, which will be compiled by the IT Advisory Committee for further processing for scrapping.

b) End-user department/section/IT Advisory Committee will prepare "IT equipment condemnation note" in the pro-forma attached as Annexure-I.

c) Department/section/Technical Cell will constitute a condemnation committee which will review the condemnation notes and recommend the condemnation of equipment as per approved guidelines. The Committee should have at least one member from the Technical Cell (for proposals initiated by department/section) and one from the finance wing.

d) All procedures and rules of the government on maintenance of records for condemnation of non-consumable items will be adhered to in these cases.

e) The condemnation report so prepared shall be put up for approval. The condemnation will be done only after recommendation of the IT committee and approval is obtained from competent authority.

# 7. Role and Responsibilities

## 7.1 Responsibilities of TECHNICAL CELL:

### A. Campus Network Backbone Operations:

a. The campus network backbone and its active components are administered, maintained and controlled by TECHNICAL CELL.

b. TECHNICAL CELL operates the campus network backbone such that service levels are maintained as required by the University Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

### B. Physical Demarcation of Campus Buildings' Network

a. Physical connectivity of campus buildings already connected to the campus

network backbone is the responsibility of TECHNICAL CELL.

b. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of TECHNICAL CELL. It essentially means exactly at which location the fiber optic-based backbone terminates in the buildings will be decided by the TECHNICAL CELL. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of TECHNICAL CELL.

c. TECHNICAL CELL will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.

d. It is not the policy of the University to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the University's Internet links.

**C. Network Expansion:** Major network expansion is also the responsibility of TECHNICAL CELL. Every 3 to 5 years, TECHNICAL CELL reviews the existing networking facilities, and needs for possible expansion. Network expansion will be carried out by TECHNICAL CELL when the university makes the necessary funds available. As IT is the essential component for everyday life of University, funds shall be radially available.

**D. Wireless Local Area Networks:** Where access through Fiber Optic/UTP cables is not feasible, in such locations TECHNICAL CELL considers providing network connection through wireless connectivity.

**E. Providing Net Access IDs and email Accounts:** TECHNICAL CELL provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the university upon receiving the requests from the individuals.

**F. Network Operation:** TECHNICAL CELL is responsible for the operation of a centralized Network Operation. The campus network and Internet facilities are available 24/7 a week. All network failures and excess utilization are reported to the TECHNICAL CELL technical staff for problem resolution.

**G. Network Policy and Technology Standards Implementation:** TECHNICAL CELL is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

**H. Receiving Complaints:** TECHNICAL CELL may receive complaints from the users if any of the users is not able to access the network due to a network related problem at the user end. Such complaints may be generally through phone call/Mail/Complain Register to TECHNICAL CELL. The designated person in TECHNICAL CELL receives complaints from the users and coordinates with the user/service engineers or with the internal technical team to resolve the problem within a reasonable time limit. TECHNICAL CELL will be responsible only for solving the network related problems or services related to the network. TECHNICAL CELL may also receive suggestions for the smooth and timely delivery of services.

**I. Disconnect Authorization:** TECHNICAL CELL will disconnect any section, department or division for routine maintenance for networking and its related issues. TECHNICAL CELL will be constrained to *disconnect any Section, department, system or division from the campus network backbone* whose traffic violates practices set forth in this policy or any network related policy. If a Section, department, or division is disconnected, TECHNICAL CELL shall inform the concerned and shall provide the conditions that must be met to be reconnected.

**J. Enforcement:** TECHNICAL CELL periodically scans the University network for provisions set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines. Such disconnection shall be informed to the concerned individual and shall also be informed on conditions for reconnection. In case of disconnection or major fault the IT cell shall inform the departments through mail or bulk messages regarding disconnection and reconnection.

**K.** The TECHNICAL CELL (In charge) will be responsible for allocation of roles to the personnel under technical cell for better functioning of IT related issues in CUJ.

**L.** Where feasible, Technical Cell Head is to enforce these policies by System Configuration.

**M.** Backing up Critical data and application residing on Servers while ensuring safe custody and accounting of media used for it.

**N.** All the computers that were purchased by the university centrally shall be handed over to the Technical Cell. Technical Cell will then receive the requisition and distribute, and Technical Cell will also attend the complaints related to any maintenance related problems.

## 7.2 Responsibilities of Department or Sections

A. Any Centre, department, or Section or other entity can connect to the University network

using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the university. The user account will be provided by TECHNICAL CELL, upon filling up the prescribed application form and submitting it to TECHNICAL CELL.

B. Each Section, department, or division should identify at least one person as a Point of Contact and communicate it to TECHNICAL CELL so that TECHNICAL CELL can communicate with them directly in case of any network/system related problem at its end.

C. For any defective data storage device/IT assets like hard drive, pen drive etc are to be physically destroyed before dumping or throwing.

## 7.3 Responsibilities of the Administration

TECHNICAL CELL needs latest information from the different Administrative Units of the University for providing network and other IT facilities to the new members of the university and for withdrawal of these facilities from those who are leaving the university, and also for keeping the CUJ web site up-to-date in respect of its contents.

The information that is required could be broadly of the following nature:

- Information about New Appointments/Promotions.
- Information about Superannuation / Termination of Services, or about someone who is no more a part of university due to any other reason
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Any action by the university authorities that makes individuals ineligible for using the university's network facilities.
- Information on Important Events/Developments/Achievements.

Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy should be sent to TECHNICAL CELL.

# 8. Policy Monitoring

## 8.1 Policy Dissemination

**a.** The IT Committee of the Central University of Jharkhand should ensure proper dissemination of this policy.

**b.** The IT Committee may use newsletters, banners, bulletin boards etc. to facilitate increased awareness about this policy amongst their users.

**c.** Orientation programs for new recruits shall include a session on this policy.

**d. For implementation of this policy, the IT cell shall be competent to suggest modifications in rules and the University will amend necessary rules as**

**suggested by IT cell or otherwise from time to time.**

### 8.2 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. Access Control Policy: Without permission mobile phones or any gadgets or electronic photography devices are not allowed in restricted or prohibited areas or in confidential documents rooms. Users are encouraged to be vigilant and to report any suspected violation of this policy immediately to the concerned office.

### 8.3 Review and Monitoring of Policy:

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.

Review of this policy document shall be done by a committee chaired by the Vice Chancellor or his Nominee of the University and all the members of the IT Committee. The University reserves all rights to relax the terms of this policy, further when required review of this policy document shall be done by committee.

### 8.4 Change Management

IT Policy necessarily evolves with changes in IT infrastructure and threat scenario. Once promulgated, further changes in IT policy would be reflected as additions/deletions to this document. Anything that is not covered in this policy will be decided by the Vice Chancellor. The Vice Chancellor has authority to interpret this policy and any decision taken by the Vice Chancellor will be final and binding on everyone.

## 9. Committee

### 9.1 **The IT Committee**

The IT Committee shall be an apex advisory and recommending body on all matters pertaining to IT in the University and shall report to competent authority. It shall be mandatory for Technical Cell to seek recommendation on all matters pertaining to University IT planning, maintenance, procurement and disposal prior to putting forward the proposal to competent authority. Investigators/co-investigators, planning to acquire and manage IT assets as well as department/section, who intend to develop and manage IT resources within the department may seek assistance from IT Committee.

The IT Committee shall consist of

- Registrar as Chairperson,
- Director IQAC,
- Technical Cell (In charge) as Secretary,

- System Analyst – (Member),
- Senior Technical Assistant (Technical Cell) – Member Secretary.
- Two Professor from the University,
- One faculty from DCST,
- One officer not below the rank of Under Secretary (to be decided by competent authority) as members, preferably from the departments/ section/ units, who are the major user of IT resources/ services.

The committee may invite or co-opt additional members from outside as per need with the permission of Chairperson.

## 9.2 Function:

The Department/ Centre Committee shall have the following functions, namely–

(a) to advise and recommend on proposals for the development & procurement of new infrastructure, software, computers and other IT equipment for university end-user, students and for the general-purpose computer labs;

(b) To evaluate & advise on proposal for annual maintenance;

(c) To advise and recommend on proposals of ERP/intranet, ICT equipment & Smart boards, design and development of website and portals;

(d) The committee shall provide advice on IT facilities/ software/ hardware/ internet/ Wi-fi access for the University as well as matters pertaining to planning, purchase, utilization, maintenance and disposal.

## 9.3 Meetings:

Meetings of the IT Committee shall be convened at least twice in a year by the Chairperson.

At the end of the financial year, Technical Cell shall submit to the IT Committee a copy of annual statement of expenditure on IT items, and newly added and disposed stocks for better planning and assessment of status of IT infrastructure in the campus.

The proceedings of the IT Committee shall be submitted to the competent authority.

**9.4. Others:**

9.4.1. The IT policy of the CUJ respects the right to privacy of every individual concerned.

9.4.2. The IT cell will have the mandate to spread awareness regarding cyber fraud, password protection etc.

9.4.3. The vacancies in the IT cell shall be reviewed and filled on priority basis.

9.4.4. As NEP2020 has special focus on Indian languages, IT cell shall take necessary steps to help all concerned departments to implement it subject to the resources available.

Annexure1

# Central University of Jharkhand

*Main Campus (Cheri-Manatu), Ranchi, Jharkhand*

## Application for E-Mail account for Student/ Research Scholars

| Please fill out the relevant sections in BLOCK LETTERS for requested service | |
|---|---|
| Request Date: | Department: |
| Contact Tel: | Present Email: |

**Type of Email ID Requested:** Student (Individual)/ Conference/ Seminar/ Others

(Email ID Format – firstname.registrationnumber@cuj.ac.in)

**Name:** ..... **Course:** .....

**Registration no. :** ..... **Session:** .....

**Start of Course** (MM/ YYYY): ..... ..... ...

**End of Course** (tentative) (MM/ YYYY): .....

*Declaration:* I hereby confirm that the information provided herein is accurate, correct, and complete. I also confirm I will strictly use the email id for academic and research purpose only. I am aware that I will be using the email ID till the completion of the course, and it will be suspended/ deleted thereafter. Also, I will be abiding by the existing and forthcoming terms and condition of using email ID of CUJ domain.

**Signature of the Applicant**

**AUTHORIZATION by DEPARTMENT:** (Date stamp required)

Name: Head/ Coordinator:

Date:

Please Note: By authorizing the above request, you agree to notify the Technical Cell *immediately*, *if* any student leaves the University *either by* course completion or transfer, discontinuation etc.

**Official Use Only** (To be filled by Technical Cell)

| Date of Account Activated: | Official Signature: |
|---|---|
| | |

Annexure – 2

# Central University of Jharkhand

*Main Campus (Cheri-Manatu), Ranchi, Jharkhand*

## Application for E-Mail account for Contractual Faculty

| | |
|---|---|
| Please fill out the relevant sections in BLOCK LETTERS for requested service | |
| Request Date: | Department: |
| Contact Tel: | Present Email: |

**Type of Email ID Requested:** Contractual Faculty (Individual)

(Email ID Format –firstname.**department**@cuj.ac.in)

**Name:** …… **Department:** ……

**Date of Joining:** ……

**Date of end of service in CUJ:** ……..

**Declaration**:I hereby confirm that the information provided herein is accurate, correct, and complete. I also confirm I will strictly use the email id for academic and research purpose only. I am aware that I will be using the email ID till my tenure at CUJ, and it will be suspended/ deleted immediately thereafter. Also, I will be abiding by the existing and forthcoming terms and condition of using email ID of CUJ domain.**I have attached my offer letter and duly approved joining report with this form.**

**Signature of the Applicant**

**AUTHORIZATION by DEPARTMENT: (**Date **stamp** required**)**

Name of Head/ Coordinator: Sign of Head/ Coordinator:

Date: Seal:

**Please Note:** By authorizing the above request, you agree to inform the Technical Cell***immediately by email***, *if* any contractual faculty leaves the University *either by* end of contract or transfer, discontinuation *etc*.

**Endorsement by Registrar**

Date: **Signature:**

**Official Use Only (To be filled by Technical Cell)**

| | |
|---|---|
| Date of Email ID Account Activated: | Date of Deactivation of email ID: |
| Official Signature: | Official Signature: |

Annexure -3

झारखण्ड केन्द्रीय विश्वविद्यालय

**CENTRAL UNIVERSITY OF JHARKHAND**

**(Established by an Act of Parliament of India in 2009)**

**Homepage: http://www.cuj.ac.in**

Paste your recent size photograph

## INTERNET ACCESS REQUEST FORM FOR STUDENTS

Student Registration Number _____ Program Name _____

Department _____

Internet use Justification _____

**Personal Details**

Name _____

Father name _____

Date of Birth _____ Nationality _____

Gender _____ Marital Status _____

Category _____

Email ID _____

**Permanent Address**

State _____ Pin Code _____

**Address for Correspondence**

Same as above

State _____ Pin Code _____

*Emergency Phone No. _____ Blood Group _____

The information given by me in this application is correct and true. **I will be held responsible for any kind of internet use misconduct from my user id.**

Forwarded by controlling officer/Section Head Signature of the Student _____

User ID _____

Annexure - 4

# CENTRAL UNIVERSITY OF JHARKHAND
## IT SERVICE REQUEST FORMAT (A)

| **CENTRAL UNIVERSITY OF JHARKHAND**<br>**IT SERVICE REQUEST FORMAT (B)** |
|---|
| Name of Department/ Section: Date: |
| Name of the University Official (Client): |
| Description of problem (from the client side): |
| Description of problem (as per Technical Cell) after investigation: |
| Resources used to resolve the problem: |
| Name of staffs (of Technical Cell):<br>Signature of the staff(s) |
| Remarks/ comments from the University Official (Please marks specifically regarding the completion of work in temporary/ permanent basis and your satisfaction after resolving the problem):<br>Signature by University official (with date) |