IT POLICY AND CYBER SECURITY POLICY

Version: 1.0

Central University of South Bihar
Gaya

2022

Table of Contents

Abbreviations used in the document

Abbreviation	**Full Form**
IT	Information technology
IoT	Internet of Things
ICT	Information and Communications Technology
UCC	University Computer Center, which is the IT section of the University
UITC	University IT Services Advisory Committee, which is an apex advisory and recommending body on all matters pertaining to IT in the University
OSS	Open Source Software or freeware software
CSS	Commercial Source Software, also called commercial software
AMC	Annual maintenance contract
CUSB	Central University of South Bihar
MeitY	Ministry of Electronics and Information Technology
DeitY	Ministry of Electronics and Information Technology

[1] University Policy on IT and Cyber Security

"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 whenever 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 CUSB IT & Cyber security 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 situation, the policy document addresses e-education needs and ensure preparedness for implementation of hybrid mode of learning."

About Information Technology (IT) and Cyber Security Policy

Central University of South Bihar extensively provides a variety of IT recourses to carry out its business and facilitate in teaching, academics, administrative and financial activities. IT, ICT, IoT devices, softwares, networks and email facility, social media platforms have been employed for wide ranging work from administrative tasks, services and financial transactions to information dissemination, outreach, support, training and better learning environment for students. In view of significant utilization of IT resources and cyber activities in almost every business, it is imperative to provide a secure digital environment for financial transaction, to protect infrastructure such as software, ebooks and periodicals and to preserve confidentiality. It is also imperative to ensure optimum utilization of government resources and to make data available for better learning, for great transparency and information dissemination.

Proposed policies of the MeitY and other Governmental bodies

Various polices have been laid down by the concerned Ministry of Electronics and Information Technology (MeitY) for all governmental and semi-governmental organizations on various aspects of use of IT resources and cyber security. Accordingly, the following Policies and Guidelines of MeitY have been adopted in Central University of South Bihar (CUSB), which forms the first part of IT and cyber security Policies of CUSB. University Computer Center (UCC), which is an IT section in the University is the nodal and implementing agency on these policies in the University.

- *Policy and Guidelines on the Use of IT Resources & Devices* (as per MeitY - F. No. 2(22)/2013-EG-II and amendments/ modification there off from time to time).
  The policy governs the usage of IT Resources from an end user's perspective. Guidelines supports the implementation of this policy by providing the best practices related to use of IT devices such as desktop, laptops, and peripheral devices and components, ICT and IoT devices such as Smart Board, Various Lab equipments etc.

- *E-mail, password and security Policy* (as per MeitY - F. No. 2(22)/2013-EG-II and amendments/ modification there off from time to time)
  This governs the usage of email services provided to students, scholars, faculties, staffs and visitors.

- *Policy on Adoption of Open Source Software* (as per MeitY - F. No. 1(3)/2014 – EG II and amendments/ modification there off from time to time)
  The aim of the policy is to encourage the adoption and use of Open Source Software (OSS) in academia

In addition, relevant measures would be taken to ensure that MeitY's common guidelines on National Cyber Security Policy-2013 (NCSP-2013) and Guidelines for Adoption of Electronic Payments and Receipts (EPR: 01 Version: 1.0 November, 2016) is followed.

For fair and optimum procedures of procurement, distribution and utilization of IT resources in safe and appropriate manner as per the financial rules, following policies are also in place in the University, which forms the second part of the policy

.

- *IT asset Procurement, distribution, maintenance, inventory and disposal policy*

At the end, the policy document contains various forms and formats for implementation and usage of IT resources and allocation.

[2]. Policy on the Use of IT Resources

1. Introduction
   1.1.1. CUSB 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 CUSB. It is, therefore, expected that these resources are used primarily for CUSB' related purposes and in a lawful and ethical way.

2. Scope
   2.1. This policy governs the usage of IT Resources from an end user's perspective.
   2.2. This policy is applicable to all end-user of CUSB.

3. Objective
   3.1. The objective of this policy is to ensure proper access to and usage of IT resources and prevent their misuse by the users. Use of resources provided by CUSB imply the user's agreement to be governed by this policy.
4. Roles
   4.1. The official identified for the following task would be responsible for the management of the IT resources deployed for the use of entire user base under their respective domain
      4.1.1. Competent Authority - Registrar
      4.1.2. Designated Nodal Officer – System Analyst as Nominated by Implementing Authority
      4.1.3. Implementing Department – University Computer Center (UCC)

5. Access to the Network

5.1. Access to Internet and Intranet

a. A user should register the client system and obtain one time approval /permission from the Implementing authority before connecting the client system to the CUSB 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 implementing authority.

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 company's network.

5.2 Access to CUSB Wireless Networks

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

a. A user should register the access device and obtain one time approval / permission from the Implementing department before connecting the access device to the CUSB' wireless network.

b. Wireless client systems and wireless devices should not be allowed to connect to the CUSB' 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.

5.3 Filtering and blocking of sites:

a. Implementing Department 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. Implementing Department 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.

6. Monitoring and Privacy:

6.1. CUSB shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

6.2. CUSB, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on devices under intimation to the user. This includes items such as files, e-mails, and Internet history etc.

7. e-mail Access from the CUSB Network

7.1. Users should refrain from using private e-mail servers from University network.

7.2. e-mail service authorized by the CUSB and implemented by the Implementing Department should only be used for all official correspondence. For personal correspondence, users may use the name-based e-mail ID assigned to them on the CUSB authorized e-mail service.

More details in this regard is provided in the "e-mail Policy of CUSB".

8. Access to Social Media Sites from CUSB Network
   8.1. Use of social networking sites by end-user is governed by "Framework and Guidelines for the use of Social Media for Government of India Organizations" available at http://deity.gov.in.
   8.2. User should comply with all the applicable provisions under the Government Laws, while posting any data pertaining to the CUSB on social networking sites.
   8.3. User should adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, discrimination, harassment and other applicable laws.
   8.4. User should report any suspicious incident as soon as possible to the Implementing authority.
   8.5. User should always use high security settings on social networking sites.
   8.6. User should not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
   8.7. User should not disclose or use any confidential information obtained in their capacity as an end-user /contractor of the organization.
   8.8. User should not make any comment or post any material that might otherwise cause damage to the organization's reputation.

9. Use of IT Devices Issued by CUSB
   9.1. IT devices (Desktops, Printers, Scanners, iPads, Standalone PCs) issued by the CUSB to a user should be primarily used for Official purposes and in a lawful and ethical way and should be governed by the practices defined in the document "Guidelines for Use of IT Devices on CUSB Network" Under the caption "Policy on Use of IT Resources".

10. Responsibility of CUSB

10.1 Policy Compliance

a. CUSB shall implement appropriate controls to ensure compliance with this policy by their users. Implementing Departments shall provide necessary support in this regard.
b. A periodic reporting mechanism to ensure the compliance of this policy shall be established by the competent authority of the organization.
c. Nodal Officer shall ensure resolution of all incidents related to the security aspects of this policy by their users. Implementing Department shall provide the requisite support in this regard.
d. Competent Authority of the user organization shall ensure that training and awareness programs on use of IT resources are organized at regular intervals. Implementing Agency shall provide the required support in this regard.

e. Users should not install any network/security device on the network without consultation with the Implementing Department.

10.2 Policy Dissemination

a. Competent Authority shall ensure proper dissemination of this policy.
b. Competent Authority may use newsletters, banners, bulletin boards, corporate Websites and Intranet etc. to increase awareness about this policy amongst their users.
c. Orientation programs for new students/recruits should include a session on this policy.

11. Security Incident Management Process

11.1. A security incident is defined as any adverse event that can affect the availability, integrity, confidentiality and authority of data owned by CUSB.

11.2. Implementing Department reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority.

11.3. Any security incident noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the Implementing Department.

12. Scrutiny/Release of logs

12.1. Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the Implementing Department shall be done as per the Government Laws and other applicable laws.

12.2. Implanting department shall nether accept not act on the request from any other organization save as provided in this clause, for scrutiny of release of logs.

13. Intellectual Property

13.1. Material accessible through the network and resources of CUSB shall be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users should not use the network and resources of CUSB in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

14. Enforcement

14.1. This policy is applicable to all end-user of CUSB as specified in clause 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.

14.2. Each department, centre, section and unit should be responsible for ensuring compliance with the provisions of this policy. The Implementing Departments would provide necessary technical assistance in this regard.

15. Deactivation

15.1. In case of any threat to the security of the systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the Implementing Department.

15.2. Subsequent to such deactivation, the concerned user and the Competent authority of that organization should be informed.

[3] Guidelines for Use of IT Resources & Devices

1. Introduction
   1.1. CUSB has formulated the **"Policy on Use of IT Resources"**. This document supports the implementation of this policy by providing the best practices related to use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners.

2. Desktop Devices

   2.1. Use and Ownership
      2.1.1. Desktops should normally be used only for transacting official work. Users should exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

   2.2 Security and Proprietary Information
      a. User should take prior approval from the competent authority of CUSB to connect any access device to the network.
      b. User should keep their passwords secure and not share their account details. User shall keep strong and secure passwords as the password policy.
      c. All active desktop computers should be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.
      d. Users should ensure that updated virus-scanning software is running in all systems. Users should exercise due caution when opening eMail attachments received from unknown senders as they may contain malicious software.
      e. User should report any loss of data or accessories to the UCC.
      f. User should obtain authorization from the competent authority before taking any CUSB-issued desktop outside the premises.
      g. Users should properly shut down the system before leaving the office.
      h. Users should encrypt all sensitive information while while storing it on the desktop.
      i. By default all interfaces on the client system should be disabled and those interfaces that are required are enabled.
      j. Booting from removable media should be disabled.
      k. Users should be given an account with privileges on the client systems. User should not be given administrator privileges, excepting where required on a temporary basis.
      l. Users should abide by instructions or procedures as directed by the UCC from time to time.
      m. If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be immediately reported to the UCC for corrective action.
      n. Any Annual Maintenance Contract with service providers should include a clause that Hard Disk should be retained by the CUSB, even if it is faulty. While disposing the Hard disk it should be destroyed so that data cannot be retrieved.

2.3 Use of software on Desktop systems

a. Users should not copy or install any pirated/illegal software on their own on their desktop systems.
b. A list of allowed software should be made available by the Implementing Department. Apart from the Software mentioned in the list, any addition to the list by the respective departments/units/sections/centers should be done under intimation to UCC.

2.4 Sharing of data

a. Users should not share their account(s), passwords, security tokens (i.e. smartcard), Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

2.5 Use of network printers and scanners

a. User should use a strong administrator password on the device to help defend against attacks and to prevent re-configuration by an unauthorized user.
b. Where the device supports Access Control Lists (ACLs), the devices should be configured to block all traffic from outside the Network IP range.
c. FTP and telnet server on the printer should be disabled.
d. User should disable any protocol or service not required.

3. Use of Portable devices

Devices covered under this section include CUSB- issued laptops, mobiles, iPads, tablets, PDAs etc. Use of the devices should be governed by the following:

a. User should be held responsible for any unauthorized usage of access device issued by CUSB by a third party
b. Users should keep the devices issued by CUSB with them at all times or store them in a secure location when not in use. User should not leave the devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).
c. User should ensure that the portable devices are password protected and auto lockout enabled.
d. Users should be given an account with privileges on the client systems. User should not be given administrator privilege excepting where required on a temporary basis.
e. User should ensure that remote wipe feature is enabled on the CUSB issued device, wherever technically feasible. Users should not circumvent security features on their devices.
f. The concerned nodal officer of CUSB should ensure that the latest operating system, centralized anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls should be enabled.
g. Users should wipe or securely delete data from the device before returning/ disposing it off.
h. Lost, stolen, or misplaced devices should be immediately reported to the Implementing Department and the competent authority.
i. Data transmissions from devices to the services on the CUSB network should be over an encrypted channel.
j. When installing software, user should review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

4. External Storage Media:

Devices covered under this section include CUSB issued CD/DVD's, USB storage devices etc. Use of these devices should be governed by the following:

a. It is advisable that the use of external storage media, by default should not be allowed in the CUSB network.
b. Users should use only the media, if issued by the organization, for all official work. The user should be responsible for the safe custody of devices and content stored in the devices which are in their possession.
c. Classified data should be encrypted before transferring to the designated USB device. The decrypting key should not exist on the same device where encryption data exists
d. Classified/ sensitive information should be stored on separate portable media. User should exercise extreme caution while handling such media.
e. Unused data on USB devices should be cleaned through multiple pass process (like wipe/eraser software)
f. Users should not allow USB device belonging to outsiders to be mounted on CUSB systems.

4.1 Use of External storage media by a visitor

a. Visitors shall not be allowed to carry any portable media without permission.
b. If it is necessary to allow the visitor to use a USB memory device for any reason, it should be used only on designated systems meant for specific purposes. The USB device belonging to visitors should be mounted on systems that are connected and belong to the network of CUSB.

4.2 Authority issuing External storage

a. Competent Authority of the CUSB shall ensure that process is in place to maintain records for procurement, issue, return, movement and destruction of the storage devices.
b. All obsolete USB devices should be physically destroyed to avoid misuse.

[4] E-mail, password and security Policy

[a]. E-mail Policy

1. Introduction
   1.1 The University uses e-mail 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.
   1.2 This policy of Central University of South Bihar lays down the guidelines with respect to use of CUSB e-mail services. The Implementing Department of University E-mail Service shall be the UCC, CUSB.
   1.3 This policy is based on the E-mail Policy adopted by Govt. of India, vide October 2014, Version 1.0, with suitable changes.

2. Scope
   2.1 Only the e-mail services provided by G-Suite (www.cusb.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.
   2.2 This policy is applicable to all end-user / research students of CUSB 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.
   2.3 E-mail can be used as part of the electronic file processing in university.

3. Objective
   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 CUSB e-mail service amounts to the user's agreement to be governed by this policy.
   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 Any other policies, guidelines or instructions on e-mail previously issued shall be superseded by this policy.

4. Role specified for implementation of the Policy
   The following roles are specified in each department using the university e-mail service. The official identified for the task shall be responsible for the management of the entire user base configured under that respective domain.
   4.1 Competent Authority shall be the the Registrar, CUSB.
   4.2 Designated Officer of Department/Centre as identified by the Competent Authority.
   4.3 Only the implementation agency i.e. UCC, CUSB is authorized to exempt any Department/ Official as per Clause 12 of this policy.

5. Basic requirements of CUSB e-mail Service
   5.1 Security
   a) Considering the security concerns with regard to a sensitive deployment like e-mail, apart from the service provided by the UCC, there would not be any other e-mail service under the university.
   b) All departments/centres/section/units, except those exempted under clause 12 of this policy, should migrate their e-mail services to the centralized deployment of the UCC for security reasons and uniform policy enforcement.
   c) 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.

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

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

(2) Any e-mail addressed to a user, whose account has been deactivated /deleted, shall not be redirected to another email address. Such e-mails may contain contents that belong to the university and hence no e-mails shall be redirected without the permission of competent authority.

(3) The concerned designated officer of the department/ centre/unit/section shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User.

(4) In case a compromise of an e-mail id is detected by the UCC, 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 UCC reserves the right to reset the password of that particular e-mail id under intimation to the Registrar/Vice Chancellor/ concerned designated officer of the respective Department/Centre.

(5) 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 UCC 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.

(6) Forwarding of e-mail from the e-mail id provided by university to the university official's personal id outside the CUSB email service is generally not allowed due to security reasons. Official e-mail id provided by the UCC can be used to communicate with any other user, whether private or public. However, the user must exercise due discretion on the contents that are being sent as part of the e-mail.

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

5.2 E-mail Account Management

a) Based on the request of the respective department/Centre, UCC will create two ids, one based on the designation and the other based on the name. Designation based id's 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@cusb.ac.in for one-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.

5.3 Delegated Admin Console

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

5.4 E-mail Domain

By default, the address "userid@cusb.ac.in" shall be assigned to the users. The user id shall be created as per the addressing policy of university.

5.5 Use of Secure Passwords

All users accessing the e-mail services must use strong passwords for security of their e-mail accounts. More details about the password policy are available in "Password Policy" under the section A.2b.

5.6 Privacy

Users should ensure that e-mails are kept confidential. UCC 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.

6. Responsibilities of Departments/ Centres

6.1 Policy Compliance

a) All departments/centres shall implement appropriate controls to ensure compliance with the e-mail policy by their users. UCC shall give the requisite support in this regard.

b) The department/centre shall ensure that official e-mail accounts of all its users are created only on the e-mail server of the university.

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

d) Head of Department shall ensure that training and awareness programs on e-mail security are organized at regular intervals. The UCC shall provide the required support.

6.2 Policy Dissemination

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

b) Orientation programs for new recruits shall include a session on the e-mail policy.

7. Responsibilities of Users

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/section/unit or committee.

d) Examples of inappropriate use of the e-mail service

i. Creation and exchange of e-mails that could be categorized as offensive, harassing, obscene or threatening. However, it is acknowledged that individuals, for the purpose of work/research may be required to receive/send content which may, in normal course, be categorized as offensive, harassing, or obscene. For the purpose of legitimate research, such use is permitted if appropriate permissions are obtained from the heads of the respective department/centre.

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

iii. Unauthorized access of the services. This includes the distribution of e-mails anonymously, use of other officers' user ids or using a false identity.

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

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

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

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

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

ix. Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list.

x. Use of distribution lists for the purpose of sending e-mails 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.

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 UCC shall not restore the data lost due to 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.

8. Scrutiny of e-mails/Release of logs

8.1 Logs comprise of the flow of emails but not the content of the emails. Notwithstanding anything in the clauses above, the disclosure of logs/e-mails to law enforcement agencies and other departments/centres by the UCC would be done only as per the IT Act, 2000 and other applicable laws.

8.2 The UCC shall neither accept nor act on the request from any other department/centres, save as provided in this clause, for scrutiny of e-mails or release of logs.

8.3 UCC will maintain logs for a period of two years.

8.4 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/Centre 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.

8.5 The group mail, bulk mail, mail to multiple account holders shall in general require approval of the Administrator or the concerned head/chairperson of the department/section/unit or committee before circulation.

9. Security Incident Management Process

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.

9.2 It shall be within the right of the UCC 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.

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 UCC.

10. Enforcement

10.1 This "E-mail policy" is applicable to all university end-user as specified in clause 2.2.

10.2 Each department/centre shall be responsible for ensuring compliance with the provisions of this policy. UCC would provide necessary technical assistance to the department/centres in this regard.

11. Deactivation

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 UCC.

11.2 Subsequent to deactivation, the concerned user and the competent authority of that respective department/centre shall be informed.

12. Exemption

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

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 UCC.

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.

15. Review

Future changes in this Policy, as deemed necessary, shall be made by UCC with the recommendation of UITC and approval of the competent authority.

[3] b. Password Policy

1. Purpose
   1.1. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.

2. Scope
   2.1. The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the CUSB. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

3. Policy Statements
   3.1. For users having accounts for accessing systems/services
   3.2. Users should be responsible for all activities performed with their personal user IDs. Users should not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.
   3.3. All user-level passwords (e.g., email, web, desktop computer, etc.) should be changed periodically (at least once every three months). Users should not be able to reuse previous passwords.
   3.4. Password should be enforced to be of a minimum length and comprising of mix of alphabets, numbers and special characters.
   3.5. Passwords should not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.
   3.6. All access codes including user ID passwords, network passwords, PINs etc. should not be shared with anyone, including personal assistants or secretaries. These should be treated as sensitive, confidential information.
   3.7. All PINs (Personal Identification Numbers) should be constructed with the same rules that apply to fixed passwords.
   3.8. Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.
   3.9. Passwords should not be revealed on questionnaires or security forms.
   3.10. Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.
   3.11. The "Remember Password" feature of applications should not be used.
   3.12. Users should refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.
   3.13. First time login to systems/services with administrator created passwords, should force changing of password by the user.
   3.14. If the password is shared with support personnel for resolving problems relating to any service, it should be changed immediately after the support session.
   3.15. The password should be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

4. For designers/developers of applications/sites
   4.1. No password should be traveling in clear text; the hashed form of the password should be used.
   4.2. The backend database should store hash of the individual passwords and never passwords in readable form.
   4.3. For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

5. Responsibilities:
   5.1. All individual users having accounts for accessing systems/services in the CUSB, and system/network administrators of CUSB servers/ network equipment should ensure the implementation of this policy.
   5.2. All designers/developers responsible for site/application development should ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their application.

[5] Policy on adoption of Open Source Software

1. Introduction:
   1.1. Organizations worldwide have adopted innovative alternative solutions in order to optimize costs by exploring avenues of "Open Source Software". GoI has also been promoting the use of open source technologies in the e- Governance domain within the country in order to leverage economic and strategic benefits.
   1.2. Further, the National Policy on Information Technology, 2012 has mentioned, as one of its objectives, to "Adopt open standards and promote open source and open technologies".
   1.3. In view of the above, there is a need to formulate a policy for CUSB to adopt Open Source Software. The "Policy on Adoption of Open Source Software for CUSB" (hereinafter referred to as "Policy") will encourage the formal adoption and use of Open Source Software (OSS) in CUSB.
   1.4. CUSB should endeavour to adopt Open Source Software in all technologies, as a preferred option in comparison to Closed (or Commercial) Source Software (CSS).
   1.5. The policy should be applicable to CUSB.

2. Objective
   - To provide a policy framework for rapid and effective adoption of OSS
   - To ensure strategic control in e-Governance applications and systems from a long-term perspective.
   - To reduce the Total Cost of Ownership (TCO) of projects.

3. Policy Statement
   CUSB shall endeavour to adopt Open Source Software in all e-Governance systems implemented by various Government organizations, as a preferred option in comparison to Closed Source Software (CSS). The Open Source Software shall have the following characteristics:

   3.1 The source code shall be available for the community / adopter/ end-user to study and modify the software and to redistribute copies of either the original or modified software.
   3.2 Source code shall be free from any royalty.

4. Nature of Compliance
   - Mandatory

5. Applicability
   The policy shall be applicable to all departments, sections and Units in CUSB
   - All new e-Governance applications and systems being considered for implementation.
   - New versions of the legacy and existing systems.

6. How to Comply
   6.1. All departments, sections and Units in CUSB, while implementing applications and systems should include a specific requirement in Request for Proposal (RFP) for all suppliers to consider OSS along with CSS. Suppliers should provide justification for exclusion of OSS in their response, as the case may be.
   6.2. CUSB should ensure compliance with this requirement and decide by comparing both OSS and CSS options with respect to capability, strategic control, scalability, security, life-time costs and support requirements.

7. Exception

3.1. CUSB should endeavour to adopt Open Source Software in all applications and systems implemented. However, in certain specialized domains where OSS solutions meeting essential functional requirements may not be available or in case of urgent / strategic need to deploy CSS based solutions or lack of expertise (skill set) in identified technologies, may consider exceptions, with sufficient justification.

[6] Procurement, distribution, maintenance, inventory and disposal policy

1. Procurement

A. Procurement of general purpose IT assets/items

A.1 In general, all IT assets/items to be utilized by all the section/department within the university (excluding those to be procured under externally funded projects or to be procured for department specific needs such as for department Labs or instruments) shall be processed by the UCC and the Central Purchase Committee (CPC) shall be responsible for procuring IT assets/items as per the recommendation by University IT Services Advisory Committee. No procurement shall be made without the recommendation of UITC or competent authority

A.2 General purpose software required for entire university such as operating system, anti-virus, Compilers and associated tools, Web development tools, recovery software, statistical/mathematical/computational softwares, Plagiarism-check, essential graphics, data analysis software etc. shall be recommended by University IT service advisory committee to be placed before CA for approval.

A.3 The UCC shall place the requirement of services such as AMC before UITC and upon its recommendation shall put up the proposal for Competent Authority.

B. Procurement of IT assets/Items -under externally funded projects/for Department specific Labs/instruments

B.1 It would be responsibility of investigator/co-investigator to process for procurement of essential IT assets/items and the Central Purchase Committee (CPC) shall be responsible for procuring IT assets/items. The UCC may be approached for assistance/advise in procurement of items.

B.2 Additionally, the End-user department/section/Unit may propose assets/items department/section specific needs (such as desktop/laptops for their Labs, Server/workstation/HPC machine for high-end computing) as per the requirement of the individual department/section. All such proposals for purchase of IT assets shall be directly submitted to competent authority for approval. End-user department/section shall process such proposal and the Central Purchase Section (CPC) shall be responsible for procuring IT assets/items. The UCC may be approached for assistance in procurement of items.

B.3 Softwares under externally funded project shall directly be procured by Investigators/co-investigators and need not be routed through University IT service advisory committee. Additionally, any software, specifically required for end-user department for teaching/research may be proposed and submitted to Competent authority. The UCC may be approached for assistance in procurement of items.

B.4 If investigators/co-investigator or End-user department/section/unit, if consider appropriate, may put forward the proposal with proper justification for specific AMC either at the time of purchase or later of any specific instrument/Lab to competent authority.

2. Distribution

2.1 Entitlement and modalities for the issuance of Desktop / Laptop/other IT resources to teaching and non-teaching staff members

The criteria for entitlement and procedure for issue of IT assets to University end-user is as follows:

2.1.1. Entitlement

Category	Entitlement
Faculty members (Regular position).	Laptop or Desktop, based on preference (subject to availability in the Stock)
Non-teaching Staff /Officers	Laptop or Desktop, based on preference (subject to availability in the Stock)
Non-teaching Staffs	Desktop (subject to availability in the Stock)
Faculty members (Contractual including Post-doctoral fellows/RA/Fellows and similar scientists)	Nil. (Request may be put up for approval from CA, which shall be entertained depending on the availability in the Stock)

2.1.2 It would be responsibility of investigator/co-investigator to procure/provide desktop/laptop if required to their staffs (recruited under externally funded projects) from their grant. The UCC may be approached for assistance in procurement of such items.

3. Inventory

3.1 All IT assets shall be entered in central store at the time of installation/procurement. The purchased goods will be maintained in the Central Store/concerned department, until issue. The Central store shall maintain separate record of all IT assets procured by the University or procured under externally funded projects or IT asset (such as attached computers) received along with equipment.

3.2 It shall be mandatory for the End-user department/Investigators of externally funded projects to submit the IT asset details (including those received along with Equipment) to Store section for maintain records of IT assets in the University and for facilitating coverage of such items in the AMC (post warranty period).

3.3. Dead Stock Number / Fixed Asset Number: This will be generated by the Central Store for the item issued.

3.4. Issuance: Items (excluding those procured under externally funded projects) will be issued by the Central Stores upon receipt of Requisition slip duly singed by the Dean (or Head)/ Registrar (or Deputy Registrar) for teaching / non- teaching staff respectively.

4. Installation & Maintenance

4.1. Initial Installation: It will be done by UCC/vendor. Required software like MS Windows/Linux, Antivirus software, MS Office etc., will be installed in the system by UCC. Upon user request, the UCC may assist in installation of domain specific software

4.2. Repair and Maintenance: The repair costs / items required and inventory will be worked out by UCC and the necessary records of which shall also be maintained by the UCC. Inventory / costing of repairs and maintenance will be done by UCC.

4.3. Specifications for Spare Parts will be provided to the end user by the UCC.

4.4 All IT assets, irrespective of procured by University or through external funding would be covered under AMC except those which are already covered under AMC/warranty (such

as during purchase). To save the cost of AMC, Computers/Laptop/Printers which are more than 10 years old (refer section 5 condemnation and disposa of IT assets) shall not be covered under AMC unless under exceptional circumstances as requested by the end-user with justification and duly approved by the Competent authority. Fresh tender/renewal of AMC shall require recommendation of UITC. End user seeking equipment/lab/section-specific AMC should refer section B.4.

4.5 Assets/Items not covered under AMC/not possible to repair under existing AMC, it shall be responsibility of UCC to make all possible attempt to repair the asset/item or if not possible, to facilitate/advise the end-user.

4.6 During AMC renewal/fresh tender, it would be the responsibility of Store section to provide the list of IT resources with the university upon request from UCC.

5. Condemnation & 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

5.1. Applicability

These guidelines will be applicable to all IT equipment's installed in CUSB

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.

5.2. Grounds for condemnation:

The IT equipment can be condemned on following grounds:

a) Equipment outlived its prescribed life and certified by UCC as unfit for its useful contribution. The prescribed life span of various IT equipment in general would be 10 years. Software does not require any physical scrapping.
b) Equipment which have become obsolete technology-wise and can't be upgraded and support from vendor, either paid or unpaid, does not exist and their use may result in security threat/ unauthorized access to data.
c) Beyond economical repair: When repair cost is considered too high (exceeding 50% of residual value of equipment taking depreciation into account), and the age of the equipment. Such cases should be dealt on case to case basis and should have concurrence of finance. In case of IT equipment's, a depreciation value will be calculated as per government rules.
d) Equipment that has been damaged due to fire or any other unforeseen reason and has been certified as beyond repair by the authorized service agency and agreed upon by the UCC.

5.3. Disposal:

Such equipment shall be disposed strictly following the procedure as laid down in Rule 196 to 201 of GFR 2005 and notification regarding disposal of E-Waste issued by Ministry of environment and forests. 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's/instruments shall be stopped with the effective date of scrapping. Essential data, if any, must be removed after taking proper backup and preserved by user of the equipment.

5.4. Procedure

a) Scrapping proposal will be initiated by user section/UCC, which will be compiled by UCC for further processing for scrapping.
b) End-user department/section/UCC will prepare "IT equipment condemnation note" in the pro-forma attached as Annexure-I.

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

d) All procedure 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 UITC and approval is obtained from competent authority.

[7] Committee

1 The University IT services Advisory Committee

The University IT Services Advisory Committee (UITC) 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 UCC 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 UITC or UCC.

1.1 Constitution

The University IT Advisory Committee (UITC) shall consist of Chairperson, IT Nodal officer as the secretary and faculties and officers (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 as per need.

1.2. 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's 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 matter pertaining to planning, purchase, utilization, maintenance and disposal.

1.3. Meetings of the UITC shall be convened at least twice in a year by the Chairperson.

1.4 At the end of financial year, UCC shall submit to UITC 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.

1.5 The proceedings of the UITC shall be submitted to the competent authority.

[8] Annexure

Forms and Formats

To
The Registrar
Central University of South Bihar

Photo

Subject: University Email ID and Internet / Wi- Fi Access ID

Name of Applicant:
(In Block Letter)

If you are student

Enrollment No: Session:
Centre / Department: Subject:

If you are Faculty / Officer / Office-staff

Designation:
Department:

Personal Email ID (if any):
Contact Number:

Choice of Email ID:
1. @cusb.ac.in
2. @cusb.ac.in
3. @cusb.ac.in

I hereby declare that information given above are true to the best of my knowledge and I will abide by the rules and regulations / IT policy of CUSB.

Applicant's Signature

Recommended by
Head / Head i/c of the Department / Centre

Approved
Chairman Computer Committee / Registrar

(For University Computer Centre)

Email ID created: Created on (Date):
Internet ID:

Remarks:

Created / Issued by

-: Important Instructions:-

Read the following important policies before applying for the user account/email account. By signing the application form for Wi-Fi / Net Access ID (user account)/email account / IP address allocation you agree to act in accordance with the IT policies and guidelines of Central University of South Bihar.

Failure to comply with these policies may result in the termination of your account. It is only a summary of the important IT policies of the University.

1. Wi-Fi / Net Access IDs and email Accounts: University Computer Centre provides Wi-Fi / 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 on prescribed proforma.

2. User may be aware that by using the email / ICT facility, the user is agreeing to abide by the policy of the University. It is recommended to utilize the university's e-mail services, for academic and official purpose only.

3. Using the facility for illegal/commercial purposes is a direct violation of the University's policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

4. User should not share his/her account / credential with others, as the individual account holder is personally held accountable, in case of any misuse of that Wi-Fi / Net / email account.

5. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

6. Enforcement: University Computer Centre periodically scans / checks the University computer network. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of policies and guidelines.

7. Students, staff and faculty who leave the University will have their Email ID, Net Access ID and associated files deleted (students – after 15 days, Faculty and staff – after 30 days).

8. The User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.

9. Declaration: I hereby declare that I have read the instructions given above is true to the best of my knowledge and I will abide by the rules and regulation / IT policy of CUSB as framed from time to time.

Date:.....

Place: .....

Signature of Applicant

CENTRAL UNIVERSITY OF SOUTH BIHAR

APPLICATION FOR CREATION OF INTERNET / WI-FI ID / Group Email

Photo

Name of Applicant: _____
(In Block Letter)

(A) Student

Department: _____

Programme: _____

Enrollment No: _____ Session: _____

Personal Email id : _____

Contact Number: _____

I hereby declare that information given above are true to the best of my knowledge and I will abide by the rules and regulations / IT policy of CUSB.

_____
Applicant's Signature

(B) Recommendation of the Department Head / Head i/c:

Recommended / Not Recommended

_____
Signature

(C) Technical recommendation of the University Computer Centre:

Recommended / Not Recommended

_____
Signature

(Note: Please sumbit it in Common Computer Lab)

(For University Computer Centre)

(D) Creation of Wi-Fi ID

Wi-Fi ID : _____ Date: _____

Remarks: _____ _____
Signature

(E) Addition of E-mail in Group e-mail of University

Group e-mail: _____ Date : _____

Remarks: _____ _____
Signature

-: Important Instructions:-

Read the following important policies before applying for the user account/email account. By signing the application form for Wi-Fi / Net Access ID (user account)/email account / IP address allocation you agree to act in accordance with the IT policies and guidelines of Central University of South Bihar.

Failure to comply with these policies may result in the termination of your account. It is only a summary of the important IT policies of the University.

1. Wi-Fi / Net Access IDs and email Accounts: University Computer Centre provides Wi-Fi / 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 on prescribed proforma.

2. User may be aware that by using the email / ICT facility, the user is agreeing to abide by the policy of the University. It is recommended to utilize the university's e-mail services, for academic and official purpose only.

3. Using the facility for illegal/commercial purposes is a direct violation of the University's policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

4. User should not share his/her account / credential with others, as the individual account holder is personally held accountable, in case of any misuse of that Wi-Fi / Net / email account.

5. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

6. Enforcement: University Computer Centre periodically scans / checks the University computer network. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of policies and guidelines.

7. Students, staff and faculty who leave the University will have their Email ID, Net Access ID and associated files deleted (students – after 15 days, Faculty and staff – after 30 days).

8. The User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.

9. Declaration: I hereby declare that I have read the instructions given above is true to the best of my knowledge and I will abide by the rules and regulation / IT policy of CUSB as framed from time to time.

Date:.....

Place: .....

Signature of Applicant

Central University of South Bihar

SH-7, Gaya Panchanpur Road, Village – Karhara, Post. Fatehpur, Gaya – 824236 (Bihar) Website: www.cusb.ac.in

①

(Requisition form for Laptop/ Desktop)

Name: _____

Designation: _____
(Please Select: Regular / Contractual)

Centre / Department / Section: _____

Email Id: _____ *Mobile:* _____

HOD / In-Charge *Applicant Signature*

② ----------: *(Approval)*----------

Dean / Officer in-charge

Registrar

③ ----------*Store: Record Keeping and device Issuance*----------

Model & Make of Laptop: _____ *Asset No:* _____

Serial Number: _____ *Product Number:* _____

Charger Serial Number: _____ *Laptop Bag:* _____

Signature of Store

④ ----------*For IT Section*----------

Installed Software:

Operating System (Windows)[ ] *MS-Office / Open Office* *[ ]*

Antivirus/ Quick Heal *[ ]* *Hindi-Unicode* *[ ]*

Remarks Any: ....

STA / TA

System Analyst

Guidelines for issue of Laptop / Desktop to Faculty / Officer /Staff

1. The Laptop / Desktop shall remain the property of University and it will be handed over to University as and when required.

2. Any up gradation or changes in software & hardware of the issued laptop / desktop would be carried out by University only on request of user and after due permission from the Competent Authority.

3. Any damage in software / hardware of the issued laptop / desktop would be recovered from the user.

4. It is advisable to get the laptop insured by the user at their own cost however in case of no insurance the recovery if applicable on loss/theft, shall be made from the person against whose name the laptop is issued (refer the Govt. OM No. 7(4)/E.Coord/2011 dated 10/01/2012).

5. The maintenance during warranty period will be undertaken by the company and it will be carried out at University premises only.

6. Pirated software should not be used in the laptop / desktop.

7. No sub-letting should be allowed.

I agree to the above terms and conditions as such, agree to fully cooperate with property loss reporting requirements and with property loss incident investigations.

I hereby agree to the above terms and conditions.

Signature of the user:

_____

Date: _____

----------: END: ----------

CENTRAL UNIVERSITY OF SOUTH BIHAR

Software Purchase Form

1. The indenter/purchaser may provide the ***Software Details*** such as

   Name & Type:

   Number of licence required:

   Anticipated lifetime of the software:

   Briefly describe the software's functionality. :

   List the software owned by University/department which have a similar functionality.

   Availability of Open Source software for same kind of work.

   Identify the essential differences which require this package to be purchased.

2. The indenter/purchaser may provide the ***Software Anticipated Utilizations*** such as

   Describe how the software supports your course objectives

   Courses that require the requested software (Courses codes & Titles)

   Faculty member who last taught course

   Number of students per semester

   % of class assignments that will utilize this software

   List all faculties/Research Students who would are interested in using this software

Signatures (Signatures with specific remarks)

Requestor Date:

Head/Head In-charge Date:

Central University of South Bihar, GAYA

(University Computer Centre)

Application for setup of Local WebServer (Intranet Only)

S.No.	Details	To be filled	
1	Department Name	:	
2	Name of the Custordian	:	
	Purpose	:	
3	IO Box Number	:	
4	Make of the systme	:	
5	MAC/ Physical / Adapter address	:	
6	Operation System	Win7, Win10, Linux, Solaris, If Other, specify	
7	Net-based Applicaations Runing on the System	:	
8	Whether connected directly to the LAN or through another hub / switch	YES /NO, If yes,	
		a. Directly connected to LAN	
		b. Through Hub/ Switch located in the same room / different room	
9	If the system is configured as server, services that are enabled	a. Http	h. SMTP
		b. FTP	i. Sendmail
		c. Netfs	j. MySql
		d. Network	k. SMB
		e. Nfs	l. Telnet
		f. POP3	m. Any Other,specify
		g. IMAP	
10	whether in gerneral used by single user or many users	Single / Many	
11	Which Antivirus Software is runing	:	

Date :

Signature of the Applicant

UCC Office Use Only

IP address allocated by UCC

Host Name	:
Physical / Mac Address	:
IP address	10.0.1.
Subnet Mask	255.255.255.0
Gateway	10.0.1.1
Dns Entry	14.139.5.5
	8.8.8.8

Applicant's copy

Host Name	:
Physical / Mac Address	:
Subnet Mask	255.255.255.0
Gateway	10.0.1.1
Dns Entry	14.139.5.5
	8.8.8.8

(Network Adminstrator / TA)

Systam Analyst

Central University of South Bihar, GAYA

(University Computer Centre)

Application for IP Address Allocation

No.	Details	To be filled
1	Location of the System	:
2	Identification Name of The System	School / Centre/ Department :_____ Room No. _____ Floor / Lab. No _____ Custodian By _____
3	IO Box Number	:
4	Make and Model of the System	:
5	MAC/ Physical / Adapter address	:
6	Operation System	:
7	Net-based Applicaations Runing on the System	:
8	Whether connected directly to the LAN or through another hub / switch	YES /NO, If yes, a. Directly connected to LAN b. Through Hub/ Switch located in the same room / different room
9	If the system is configured as server, services that are enabled	:
10	whether in gerneral used by single user or many users	Single / Many
11	Which Antivirus Software is runing	:

Date :

Signature of the Applicant

UCC Office Use Only

IP address allocated by UCC

Host Name	:
Physical / Mac Address	:
IP address	10.0.1.
Subnet Mask	255.255.255.0
Gateway	10.0.1.1
Dns Entry	14.139.5.5
	8.8.8.8

Applicant's copy

Host Name	:
Physical / Mac Address	:
Subnet Mask	255.255.255.0
Gateway	10.0.1.1
Dns Entry	14.139.5.5
	8.8.8.8

(Network Adminstrator / TA)

Systam Analyst

Form No:

Receipt of Returned Items / Devices in Central Store

S.No:..... **Date: ...../...../.....**

Name of the user: ....

Designation: ..... Department / Section: .....

List of Items / Devices: (To be filled by end user)

S.No.	Asset Number	Description / Accessories if any

Reason to returning the items / devices:

....

....

Signature of the user

Remarks of Technical Wing / Section:

....

....

Signature of Technical Staff

Above mentioned items / devices receipt with the consent of user:

....

Signature of Store Officer

Photocopy: 1. End User 2.Technical Wing, Original: Central Store

Central University of South Bihar, GAYA
(University Computer Centre)

OBSERVATION REPORT

(A) Asset Detail **Date:**

CUSB Asset No.:	
Model No. :	
Serial No. / Tag No. :	
Present Location / Custodian:	
Description of Complaint / Problem :	
Is it under AMC / Warranty:	Yes [ ] No [ ]

(B) Complatint Detail (From Complaint Register)

Complaint No. :		Dated :	
Compaint by :			

(C) Technical Observation

.....
.....
.....
.....

Name of Faulty Part :	
Recommendation for Replacement / Reparing:	
Estimated expenditure:	

TA / STA

Recommendation of University Computer Centre:

System Analyst

Recomendaton of University IT Advisory Committee or Chairman of Committee:

Recommended / Not Recommended

(Signature)

Remarks :

Form No:

Shifting of System / Devices

S.No:..... **Date: ...../...../.....**

Name of the user: ....

Designation: ..... Department / Section: .....

Current Location:-

Room Number: .....

Building: .....

Department / Section: .....

Allocation of System:-

Room Number: .....

Building: .....

Department / Section: .....

Reason of allocation:

....

.....

Signature of the user

Remarks of Technical Wing / Section:

....

.....

Signature of Technical Staff

Performa for Preparation of Information for Scrapping of IT Equipment (To be filled by user)

Part-A

Name of user:

.....

Designation:

.....

Section:

.....

Room no.: .....Tel. no.:

.....

Sr. No.	Item	Make & Model	Sr. No. of Item	Reason for Scrapping
1				
2				
3				
4				

(Signature of Concern user/scrapping committee members)

Part - B (To be filled by Store Section)

Sr. No.	Name of the Item with Serial no.	Date of Purchase as per Record	Purchase Cost as per Record	Asset/Stock Reg. Entry Page No.
1				
2				
3				
4				

(Signature of store section in-charge)

Part - C (To be filled by UCC)

Sr. No.	Name of the Item	Reason for scrapping	Residual Value	Any other Information/Remarks
1				
2				

(signature of UCC nodal officer)

IT-Account Withdrawal/Asset return
(for internal Use)

Check List –

1) The email account has been delisted from all the groups - Yes/No
2) The email account deleted/retained - deleted/retained for 1 month/6month/1 year/specify the period...
3) Net ID is deactivated - Yes/No
4) Received IT resources (Desktop/Laptop/accessories/any other) -

---

Acknowledgement for the User (UCC copy for record)

a. We have received items as .....and following items are remaining to be returned/lost.....
b. Your email account would be active for ..... period and after that account would be deactivated.

Acknowledgement for the User

a. We have received items as .....and following items are remaining to be returned/lost.....
b. Your email account would be active for ..... period and after that account would be deactivated.

The End

The End