

**IT Policies**  
**a) E-Mail Policy**

**ICT Section**  
**Central University of Haryana**

Dated: 21.06.2021

**Subject: - Minutes of Meeting of Committee Draft Email Policy**

A committee of following faculty members was constituted for vetting the rough draft of E-mail policy prepared by ICT Section for Central University of Haryana.

1. **Prof. Rajesh Kumar Malik**, Dean, School of Law
2. **Dr. Santosh C. Hulagabali**, Director IQAC
3. **Dr. Rakesh Kumar**, Incharge -ICT
4. **Dr. Benay K. Ray**, Coordinator-ICT

A meeting was held on 21<sup>th</sup> June 2021 at 1:00 PM in the Room No. 002, <sup>2<sup>nd</sup></sup> Floor of the Academic Block-III to discuss the draft E-mail Policy. The committee discussed the draft email policy at length and gave valuable suggestions. On the basis of the suggestions, the draft email policy for the university is updated and prepared. The updated copy of the draft email policy is attached herewith.

The meeting ended with vote of thanks to the chair.

*Benay K. Ray* 21/6/21  
(Dr. Benay K. Ray)  
Coordinator-ICT

*Rakesh Kumar*  
21-6-21  
(Dr. Rakesh Kumar)  
Incharge-ICT

*Santosh C. Hulagabali* 21/06/2021  
(Dr. Santosh C. Hulagabali)  
Director IQAC

*Rajesh Kumar Malik*  
(Dr. Rajesh Kumar Malik)  
Dean, School of Law  
21/06/2021

DRAFT

E-MAIL POLICY

CENTRAL UNIVERSITY OF HARYANA



ICT SECTION,  
Central University of Haryana,  
Mahendergarh-123031  
2021

*Anwar*

*Benny Ray*

*Rajal*

*Sankar*

## TABLE OF CONTENTS

1	Statement of Objects and Reasons	3
2	Introduction	3
3	Objectives	3
4	Scope	3
5	Specified role for implementation of the Policy	3
6	Basic requirements of University E-mail Service	4
7	Responsibilities of Departments/Centres/Sections	6
8	Responsibilities of Users	6
9	Scrutiny of E-mails/Release of logs	7
10	Security Incident Management Process	8
11	Enforcement	8
12	Deactivation of Account	8
13	Exemptions	9
14	Audit of E-mail Services	9
15	E-mail Account and Resultant Record	9
16	Review	9
17	Glossary	10

Bunoy Roy

~~Dyalu~~

Prakash

Dhruv

## 1. STATEMENTS OF OBJECTS AND REASONS

- 1.1 The Policy is required to ensure the proper use of Email facility of by all the stake holders of the university. The policy is obligatory to prevent the cyber-crimes by all those who are concerned with the university.
- 1.2 The policy is to drafted at the institutional level to implementing E-mail Policy of Government of India in letter and spirit, Hence the draft policy is in consensus with Email Policy of Government of India, October 2014 version 1.0 published and notified by Department of Electronics and Information Technology, Ministry of Communication and Information Technology, Government of India New Delhi-110003.

## 2. INTRODUCTION

- 2.1 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.
- 2.2 This policy of Central University of Haryana lays down the guidelines with respect to use of CUH e-mail services. The Implementing Department of University E-mail Service shall be the ICT Section, CUH.
- 2.3 This policy is based on the E-mail Policy adopted by Govt. of India, vide October 2014, Version 1.0, with suitable changes.

## 3. OBJECTIVES

- 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 CUH e-mail service amounts to the user's agreement to be governed by this policy.
- 3.2 All services under e-mails are offered free of cost to all officials/faculty under Departments/Centres and Research Scholars (PhD & M.Phil. Only) enrolled in the University.
- 3.3 Any other policies, guidelines or instructions on e-mail previously issued shall be superseded by this policy.

## 4. SCOPE

- 4.1 Only the e-mail services provided by G-Suite (www.cuh.ac.in), of Google shall be used for official communications by the university. Every staff, faculty member, and research student/scholar (not the students studying UG/PG/others) 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.
- 4.2 This policy is applicable to all employees and research student/scholar (not the students studying UG/PG/others) of Central University of Haryana. The directives contained in this policy must be followed by all of them with no exceptions.
- 4.3 E-mail can be used as part of the electronic file processing in university.

## 5. SPECIFIED ROLE 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.

- 5.1 Competent Authority shall be the Vice-Chancellor and the Registrar, CUH.

Biswajit Ray

Som Prakash

3  
Prakash

Sharma

- 5.2 Designated Officer of Department/Centre/Section as identified by the Competent Authority.
- 5.3 Only the implementation agency i.e. ICT Section, CUH is authorized to exempt any Department/ Official as per Clause 12 of this policy.

6. **BASIC REQUIREMENTS OF CUH E-MAIL SERVICE**

6.1 **Security**

- a) Considering the security concerns with regard to a sensitive deployment like e-mail, apart from the service provided by the ICT Section, there would not be any other e-mail service under the university.
- b) All departments/Centres/Sections, except those exempted under clause 12 of this policy, should migrate their e-mail services to the centralized deployment of the ICT SECTION 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.
- (3) The concerned designated officer of the department/ Centre 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 ICT SECTION, 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 ICT SECTION 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 ICT SECTION 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 Registrar/Vice-Chancellor and the concerned designated officer of the Department/Centre subsequently. SMS shall be one of the prime channels to contact a user;

Step 1

Bruno Ray

01/07

Sharma

- hence all users should ensure that their mobile numbers are updated.
- (6) Forwarding of e-mail from the e-mail id provided by the university to the university official's personal id outside the CUH email service is not allowed due to security reasons. Official e-mail id provided by the ICT SECTION 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.

## 6.2 E-mail Account Management

- a) Based on the request of the respective department/ Centre, ICT SECTION 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 resign or superannuate after rendering at least 20 years of service shall be allowed to retain the name-based e-mail address i.e. userid@cuh.ac.in for one-year post resignation or superannuation. After one year, the email ID is automatically suspended without taking/keeping backup of the same at ICT Section. Hence it is the responsibility of such employee to keep back up of his/her email ID. This will not apply to the users who has rendered services less than 20 years.

## 6.3 Delegated Admin Console

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

## 6.4 E-mail Domain

By default, the address "userid@cuh.ac.in" shall be assigned to the users. The user id shall be created as per the addressing policy of university. The user id of research scholars shall be created with combination of the name and roll number of the scholar for e.g. "user18000@cuh.ac.in".

## 6.5 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 caption "E-mail Policy" at <http://www.cuh.ac.in/admin/uploads/files/IT%20security%20Policy%20CUH.pdf>

## 6.6 Privacy

Users should ensure that e-mails are kept confidential. ICT SECTION 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

Bruno Ray

information in emails.

## 7. RESPONSIBILITIES OF DEPARTMENTS/CENTRES/ SECTIONS

### 7.1 Policy Compliance

- a) All departments/Centres/ Sections shall implement appropriate controls to ensure compliance with the e-mail policy by their users. ICT SECTION shall give the requisite support in this regard.
- b) The department/Centre/Sections 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) /Incharge of the department/Centres/Sections shall ensure resolution of all incidents related to the security aspects of the e-mail policy. ICT SECTION shall give the requisite support in this regard.
- d) Head of Department /Incharge shall ensure that training and awareness programs on e-mail security are organized at regular intervals. The ICT Section shall provide the required support.

### 7.2 Policy Dissemination

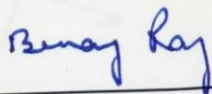
- a) Head of Department (HoD) /Incharge of the concerned department/Centres/Sections should ensure dissemination of the e-mail policy.
- b) Orientation programs for new recruits shall include a session on the e-mail policy.

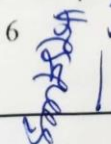
## 8. RESPONSIBILITIES OF USERS

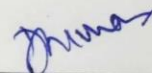
### 8.1 Appropriate Use of E-mail Service

- 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 employees' obligations towards the University as employer.
- c) Bulk emails with multiple intended recipients (viz., faculty/staff/students) shall be routed through the office of the Registrar.
- d) **Various Instances 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/Centres/Sections.
  - 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.

## 8.2 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 ICT Section does not keep any copy of email/data and hence the email/data deleted by the user's action shall not be restored by ICT Section.
  - 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 employee as well as research scholar 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.

## 9. SCRUTINY OF E-MAILS/RELEASE OF LOGS

- 9.1 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

Bruny Ray

7  
P. P. P.

S. S. S.

M. M. M.



to law enforcement agencies and other departments/Centres/Sections by the ICT SECTION would be done only as per the IT Act, 2000 and other applicable laws.

- 9.2 The ICT SECTION shall neither accept nor act on the request from any other department/Centers/Sections, save as provided in this clause, for scrutiny of e-mails or release of logs.
- 9.3 ICT SECTION will maintain the logs Admin User Activities for a period of two years.
- 9.4 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 Registrar/Vice-Chancellor and the Head of the respective Department/Centre/Sections responsible for the employee/research-scholar. 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 employee leaves the University/is terminated/dismissed from their service.
- 9.5 The group mail, bulk mail, mail to multiple account holders shall require approval of the Administrator before circulation.

#### 10. SECURITY INCIDENT MANAGEMENT PROCESS

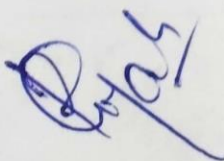
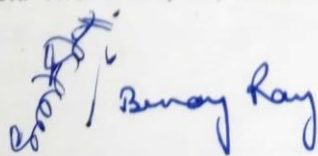
- 10.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of university data. Security incidents can be due to factors like malware, phishing, loss of a device, compromise of an e-mail id etc.
- 10.2 It shall be within the right of the ICT SECTION 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.
- 10.3 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 ICT SECTION.


#### 11. ENFORCEMENT

- 11.1 This "E-mail policy" is applicable to all university employees as specified in clause 2.2.
- 11.2 Each department/Centre/Sections shall be responsible for ensuring compliance with the provisions of this policy. ICT Section would provide necessary technical assistance to the department/Centres/Sections in this regard.

#### 12. DEACTIVATION OF ACCOUNT

- 12.1 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 ICT SECTION.
- 12.2 Subsequent to deactivation, the concerned user and the competent authority of that respective department/Centre shall be informed.
- 12.3 If the employee/researcher gets No Dues Certificate from ICT Section in case of Resignation/Relieving/completion of degree/studies from CUH, then the official email id of the employee (with cuh.ac.in extension) will be suspended after one week. Therefore, he/she will be given one-week time for taking backup of the

  Birendra Ray



email account. After this time period, the email ID is deactivated/deleted along with its data without any notice/intimation hence no queries for taking/providing backup will be entertained.

- 12.4** In case of termination/dismissal/suspension of services/ during enquires (or in any special circumstances) of the employee, the email account immediately will be suspended upon receipt of written instruction/intimation from the establishment Section/competent authorities to do so. In such case/period, the backup/access to email won't be given to such employee until the instructions are received from establishment Section/competent authorities to do so.

**13. EXEMPTIONS**

- 13.1** Departments/Centres/Sections operating Intranet mail servers with air-gap are exempted from this policy.

**14. AUDIT OF E-MAIL SERVICES**

The security audit of G-Suite email services shall be conducted periodically by committee/professional as approved by the competent authorities.

**15. 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 and have to maintain the record of such email ids.

**16. REVIEW**

Future changes in this Policy, as deemed necessary, shall be made by ICT Section with the approval of the Vice-Chancellor/Registrar/Competent Authority after due inter-departmental consultations.

Bengay Ray

~~Prady~~

Juman

~~Sanku~~

**GLOSSARY**

S.N.	TERM	DEFINITION
1	Users	Refers to Central University of Haryana employees and research scholars who are accessing the University e-mail services.
2	Implementing Department	For the purpose of this policy, the implementing department is the "ICT Section", Central University of Haryana
3	Department/ Centre/Sections	For the purpose of this policy, departments/Centres/Sections refers to all departments/offices/Centres.
4	Competent Authority	Officer responsible for taking and approving all decisions relating to this policy in the University (i.e. Vice-Chancellor and Registrar as the case may be.)
5.	Designated Officer	Officer responsible for all matters relating to this policy who will coordinate on behalf of the Department/ Centre/Sections
7	2-Step Verification	With <b>2-Step Verification</b> (also known as <b>two-factor authentication</b> ), you add an extra layer of security to your <b>account</b> . After you set it up, you'll sign in to your <b>account</b> in <b>two steps</b> using: Something you know (your password) Something you have (like your phone or a security key)
8	OTP	A <b>one-time password</b> (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords
9	POP	<b>POP</b> is short for Post Office Protocol, a protocol used to retrieve e-mail from a mail server.
10	IMAP	IMAP is short for "The Internet Message Access Protocol", a protocol used to retrieve e-mail from a remote mail server. Unlike POP, in IMAP, Messages are displayed on your local computer but are kept and stored on the mail server. IMAP allows you to sync your folders with the e-mail server which is not possible using POP.
11	Deactivation of Account	<b>Deactivation</b> of an account means that the account can no longer be accessed along with its backup data. All e-mails sent to a deactivated account shall bounce back to the sender.
12	Phishing	<b>Phishing</b> is a fraudulent attempt, usually made through email, to steal a user's personal information. Phishing e-mails almost always tell a user to click a link that takes the user to a site from where the personal information is requested. Legitimate Departments/Centres/Sections would never request this information via e-mail. Users should never click on a link. A user should always type a URL in the browser even if the link appears genuine.
13	Intranet	An intranet is a private network that is contained within an organization. For the purpose of this policy, computers connected to an intranet are not allowed to connect to internet.

*[Handwritten signature]*

*[Handwritten signature]*

*[Handwritten signature]*

*[Handwritten signature]*

**b) IT Security Policy**



# Central University of Haryana

Jant- Pali Mahendragarh-123031

---

## IT Security Policy

### **GUIDELINES FOR NETWORK USERS:**

- **Accounts and Passwords:**

- 1) 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 for educational/official purposes. The User guarantees that the User will not share the password or Net Access ID with anyone. Network ID's will only be established for students, staff and faculty who are currently affiliated with the Central University of Haryana hence forth referred to as the University.
- 2) Students and staff who leave the University will have their Net Access ID and associated files deleted.
- 3) 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.
- 4) If any user is found violating the above mentioned guidelines then he/she will be liable for any appropriate action that the University deems fit and will be solely responsible for any further prosecution that might be initiated.

- **Limitations on the use of resources:**

- 1) On behalf of the University, the Central University Computer Center (CUCC) reserves the right to close the Net Access ID of any user whose actions limit the use of computing and network resources for other users and/or in violation of any of the terms defined in this Security Policy.

- **Computer Ethics and Etiquette:**

- 1) The User will not attempt to override or break the security of the University computers, networks, or machines/networks 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, Denial of Service (DOS), identity theft, Proxy servers and the generation of threatening, harassing,

abusive, obscene or fraudulent messages. Even sending unsolicited bulk e-mail messages, phishing and spam comes under IT Policy violation.

- 2) Spreading of unsubstantiated rumors, misinformation, inflammatory, derogatory and defamatory content against any individual/organization/university on the University's network will attract strict action as per IT Security Policy and the Indian Penal Code.
- 3) In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.
- 4) User's Net Access ID gives him/her access to e-mail, and campus computing and network resources. The use of these resources must comply with University policy.
- 5) User's electronically available information
  - a) Should not contain copyrighted material or software unless the permission of the copyright owner has been obtained,
  - b) Should not violate University policy prohibiting sexual harassment,
  - c) Should not be used for commercial purposes,
  - d) Should not appear to represent the University without appropriate permission, or to represent others,
  - e) Should not appear to represent other organizations or companies,
  - f) Should not contain material which violates pornography laws, or algorithms or software which if transferred violate laws,
  - g) Should not contain scripts or code that could cause a security breach or permit use of resources in opposition to University policy.
  - h) Should not contain copyrighted audio and video material/work of art/intellectual property without permission of copyright holder and unauthorized download of such material is strictly prohibited.

- **Data Backup, Security, and Disclaimer**

- 1) CUCC will not be liable for the loss or corruption of data on the individual user's computer and/or devices as a result of the use and/or misuse of his/her computing and network resources (hardware or software) by the user or from any damage that may result from the advice or actions of a CUCC staff member in the process of helping the user in resolving their network/computer related problems. Although CUCC make a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email Account. In addition, CUCC makes no guarantee concerning the security or privacy of a User's electronic messages.

- 2) The User agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold CUCC as part of the University, harmless for any such liability or expenses. The University retains the right to change and update these policies as required without notification to the User.
- 3) Unauthorized transmission, sharing, copying and theft of University information and data through any means by any individual is strictly prohibited and will attract strict legal action.

- **Account Surrendering:**

- 1) Retiring employees and the students leaving the university (temporarily or permanently) are advised to get their accounts (NET Access and Email) disabled by giving a written letter to Information Scientist/System Analyst. This is essential as the facility is meant only for the serving employees and the enrolled students. Further, in case the accounts are not disabled and misused by some other person unauthorized, the account holder would be legally responsible for such misuse of the account. If retiring employees and the students leaving the university (temporarily or permanently) want to retain the facility for some more period, such requests may be considered, if they are given in writing with valid justification and duly recommended by the competent authority.

- **Account Termination and Appeal Process**

- 1) Accounts on the University network systems may be terminated or disabled with little or no notice for any of the reasons stated above or for other inappropriate use of computing and network resources. When an account is terminated or disabled, CUCC will make an attempt to contact the user (at the phone number and email id they have on file with CUCC) and notify them of the action and the reason for the action. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the CUCC of the same. But, if the termination of account is on the grounds of willful breach of IT policies of the university by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may first approach the Proctor, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Dean Students' Welfare (DSW) for this purpose to review the evidence and hear reasons why an appeal should be considered. If the users concerns are still not addressed then the user may approach the Grievance Redressal Committee and if the Grievance Redressal Committee recommends revival of the account, it will be enabled. However, the decision of the Grievance Redressal Committee is final and binding.
- 2) Users may note that the University's Network Security System monitors and maintains a history of logs, if any, for each user account. In case of any termination of User Account, this history of logs will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate University authorities. The University's full text of the IT Policies and Guidelines has been put on the University's web site for the convenience of the University's community.

