

IT Policy and Procedure Manual

ICFAI Foundation for Higher Education



REGISTRAR

THE ICFAI FOUNDATION FOR HIGHER EDUCATION
(Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

IT Policy and Procedure Manual: IFHE, HYDERABAD

SNo	Content	Page No
1	General, Introduction, Purpose	2
2	Applicability, Academic Freedom, Availability of Hardware in the campus, Hardware Procurement Policy, Procurement of Desktop Computers	3
3	Procurement of Portable Computers	4
4	Procurement of Server Systems	5
5	Shifting of Computers from one location to another, Backup of data, procurement of Mobile Telephones	6
6	Procurement of Software, obtaining open source software, Policy on use of Software	7
7	Own device usage Policy	9
8	Keeping Mobile Devices Secure, Information Technology Security Policy	10
9	Privacy and Confidentiality	12
10	Technology Access, Information Technology Administration Policy	13
11	Web Site Policy	14-18
12	Online Fee Collection	18
13	Emergency Management-Information Technology	19
14	E Mail	20
15	Un Acceptable E mail Usage, Cyber and Copyright Law adherence	22
16	Responsibilities of IT Cell in IFHE, Summary	23-24
17	Appendix A	25-27



REGISTRAR

THE ICFAI FOUNDATION FOR HIGHER EDUCATION
(Deemed-to-be-University Under Section 3 of the UGC ACT,1956)



2
ICFAI FOUNDATION FOR HIGHER EDUCATION

General

1. IFHE, Hyderabad is committed to providing integrated and comprehensive technologies to enhance teaching, learning and to improve productivity. It will provide students, faculty and staff with open access to a wide range of computing resources, digital information and communication networks that are basic to the academic, research and administrative functions of the University. IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the institution which must be followed by all faculty, staff and students. IFHE IT Cell will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

2. A balanced approach between user rights and responsibilities guides this policy on the appropriate use of college information technology resources. IFHE is the official owner of its technology resources, and the University reserves the right to deny use to those who do not use them responsibly. Users must adhere to all applicable laws and University policies and to the acceptable uses of information technology as defined in this policy. It is expected that all users should adhere to the highest standards of ethics and responsibility. One's use of technology must not infringe upon the rights of other users, interfere with the normal operation of computing systems and software, or consume an unfair share of system resources.

Introduction

3. The University strives to protect the privacy of its users and supports the use of technology for the free expression of ideas. As an academic community, the students, faculty, and staff of the University must respect the privacy of data, honor intellectual property, and respect the rights of others. Users must adhere to copyright laws and guidelines, remembering that the same provisions of copyright ownership and fair use that apply in the print environment apply to digital resources. Users are required to respect license agreements controlling the copying and use of computer software, library online databases and data files such as text, audio, graphics, video, etc.

4. Those who access resources whether on campus or external to campus should do so responsibly and in a way that constitutes respectful behavior of an employee, student, and faculty. All communications whether internal or external must fall within the standards outlined in the Guiding Principles for Respectful Dialogue. Any other visitor/guest who is permitted to use the IT resources of the University has to abide by the policy document.

Purpose

5. The purpose of this document is to lay down a policy to be followed by one and all in the IFHE Hyderabad to ensure, safe and optimum use of IT infrastructure and resources available with the University. IT policy document should be read in conjunction with IT Act 2000 and IT Act 2008(Amendment).

Applicability

6. This policy applies to students, faculty, staff and anyone who ever is authorized to use these resources.

Academic Freedom

7. IFHE is committed to the free flow of ideas and the freedom of electronic speech shall be fully protected. Technology resources are fundamental to communication, learning, research, publishing, and the creation of knowledge. This Policy on the Acceptable Use of Information Technology does not hinder the free exchange of ideas which are at the core of the academic process. Faculty and staff of IFHE will adhere to academic Freedom and electronic media Ethics. The content of electronic communication, teaching, and learning materials at IFHE is not censored. However, the University reserves the right to protect itself from liabilities posed by the electronic behavior of members of the University if these behaviors are illegal or violate University policies.

8. **Availability of Hardware in the Campus.** Presently internet service is being utilized from various service providers such as TATA, VODAFONE, BSNL and JIO. Entire campus is provided with Wi-Fi facility with network speed of 1GB. Net work is provided with a robust fire wall FORTIGATE (HA), three Core switches, 13 distribution switches and access/extreme switches 120 each. 1322 PCs are exclusively available for students 333 PC for Administration and Faculty. 31 computers have been exclusively provided for the Library. Language lab is provided with 92 computers.

PART -I

HARDWARE PROCUREMENT POLICY

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

10. **Procurement of Desktop Computer Systems**

- (a) The desktop computer systems purchased must run a Windows operating system and integrate with existing hardware and software.
- (b) The desktop computer systems must be purchased as standard desktop system bundle and must be of a reputed Company, such as HP, Dell, and Acer etc.
- (c) The desktop computer system bundle must include the following items:
 - (i) Desktop tower cabinet
 - (ii) 19"LED Monitors
 - (iii) Keyboard and mouse, latest option of wireless technology will be procured


REGISTRAR
THE ICFAI FOUNDATION FOR HIGHER EDUCATION
(Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

- (iv) Windows licensed software, upgrades as available for the licensed software to be updated
 - (v) The accessories as on required basis such as, speakers, microphone, webcam, printers etc. depending on the approval from the respective Dean/Director's approval
 - (vi) Intel processor, I 5, Intel Mother Board
 - (vii) The minimum capacity of the desktop must be 1 TB
 - (viii) Processor speed should be more than 122GHz
 - (ix) Minimum 8 GB RAM , provision for further expansion
 - (x) Four USB ports out of which two should support USB 3
 - (xi) Each Computer will have a DVD drive, microphone port, etc
- (d) Any change from the above requirements must be authorized by respective Director of the College
- (e) All purchases of desktops must be supported by proper guarantee and/or warranty requirements and should be compatible with the institution's server system.
- (f) All purchases for desktops must be in line with the purchasing policy of the ICFAI Society.

11. Procurement of Portable Computer Systems

- (a) The purchase of portable computer systems such as notebooks, laptops, tablets etc. is need based and will not be procured as a routine.
- (b) Portable computer systems purchased must run compatible software as that of desktops and integrate with existing hardware of the University.
- (c) The portable computer systems purchased must be of reputed brands such as HP, Dell, Acer, etc
- (d) The minimum configuration of the portable computer system must be:
- (i) Processor speed should be more than 122 GHz
 - (ii) 4 GB RAM
 - (iii) 4 Number of USB ports
 - (iv) DVD drive, microphone port, webcam, built in speakers, etc
- (e) The portable computer system must include the Windows 10 and Upgrades as available, Microsoft Office, Adobe Reader and any other software as desired by the user. All the software loaded in a computer must be licensed and user should ensure the software remains up to date.
- (f) Any change from the above requirements must be authorized by Director of the respective College
- (g) All purchases of all portable computer systems must be supported by guarantee and/or warranty clauses and be compatible with the institution's server system.
- (h) All purchases for portable computer systems must be in line with the purchasing policy of the ICFAI Society.

ICFAI FOUNDATION FOR HIGHER EDUCATION

12. **Procurement of Server systems**

- (a) Server systems can only be purchased by a team of experts on the subject.
- (b) Server systems purchased must be compatible with all other computer hardware in the institution.
- (c) All purchases of server systems must be supported by guarantee and/or warranty clauses and be compatible with the institution's other server systems.
- (d) Any deviations from the above requirements must be authorized by the Management
- (e) All purchases for server systems must be in line with the purchasing policy of the ICFAI society.

13. **Warranty & Annual Maintenance Contract (AMC)** Desktop computers/ portable computers / Network computers, UPS systems and peripherals purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking of virus.

14. **Power Connection to Computers and Peripherals** All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

15. **Network Cable Connection** While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

16. **Procurement of computer peripherals**

- (a) Computer system peripherals include devices such as printers, scanners, external hard drives etc.
- (b) Printers should be Black and white laser Jet printers. Color printers will be provided as on required basis. Preferably, the Printers should be on LAN network on sharing basis to avoid misuse and optimum utilization.
- (c) Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.
- (d) Computer peripherals purchased must be compatible with all other computer hardware and software in the institution.
- (e) The purchase of computer peripherals need to be projected on a Note duly giving details of previous procurement and present state of the equipment. If

Page 5 of 27

M. Jayalalitha
REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

there is a buy back system for the unserviceable item held with the university, the same should be explored.

(f) All purchases of computer peripherals must be supported by guarantee and/or warranty requirements and be compatible with the institution's other hardware and software systems.

(g) Any change from the above requirements must be authorized by the Director of the College and sanctioned by the management.

(h) Un- interrupted Power Supply system (UPS) should be procured from a reputed brand and ensure switching time is crucial for selection of a particular UPS.

(i) Whenever the UPS mal functions, the battery should be checked by the AMC vendor and it is required to be procured separately. The voltage and rating of the Battery is very important for Un-Interrupted power.

(j) All purchases for computer peripherals must be in line with the purchasing policy in the financial policies and procedures manual.

17. **Shifting Computer from One Location to another** Computer system may be moved from one location to another with prior written intimation to the System Administrator IT, as they maintains a record of computer identification names and corresponding IP address.. As and when any deviation (from the list maintained by System Administrator) is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone. System will be restored only after the anomaly is rectified.

18. **Backup of Data** Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.

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

20. **Procurement of Mobile Telephones**

(a) Mobile phones have become necessity for all the important functionaries to be in communication with each other. ICFAI procurement division will decide on the model and the price of the mobile phone to be issued to an official based on the designation and requirement.

(b) Though mobile phone along with SIM card is provided by the head office, it should be judiciously utilized.

(c) Personal calls on the official phone should be avoided.

(d) Data usage as allowed by the head office can be sued, in excess to the authorized data will be charged to the individual.

ICFAI FOUNDATION FOR HIGHER EDUCATION

- (e) Only legal and permitted applications can be downloaded and installed on the Official phone.
- (f) Chinese Applications should be avoided.
- (g) Pornographic material, child pornography is illegal and individual is responsible for the content on the official phone. Legal action may be taken against downloading such illegal applications/software.
- (h) Any changes in the requirement other than the policy of ICPD will have to be authorized by the Management.

21. **Procurement of Software**

- (a) This policy provides guidelines for the purchase of software for the institution to ensure that all software used by the institution is appropriate, value for money and where applicable integrates with other technology for the institution. This policy applies to software obtained as part of hardware bundle or pre-loaded software.
- (b) All software, including licensed software, free software, and open source software must be approved by management prior to the use or download of such software.
- (c) The purchase of all software must adhere to this policy. All procurements must be from a registered dealer and through ICPD only.
- (d) All purchases of software must be supported by guarantee and/or warranty requirements and updates through internet from the OEM should be made available. Software should be compatible with the institution's server and/or hardware system.
- (e) Any changes from the above requirements must be authorized by respective Director of the College
- (f) All purchases for software must be in line with the purchasing policy of ICFAI society.
- (g) The licensed software that is available presently with the University are SAP, SAS, SPSS, WINDOWS 10, MSO 16, AUTOCAD, Rational Rose, LINUX, SOLARIS, WINDOWS SERVER 2008, 2012

22. **Obtaining open source or freeware software**

- (a) Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.
- (b) In the event that open source or freeware software is required, approval from the System Administrator must be obtained prior to the download or use of such software.
- (c) All open source or freeware must be compatible with the institution's hardware and software systems.

23. **Policy for Use of Software**

- (a) This policy provides guidelines for the use of software for all employees within the institution to ensure that all software use is appropriate. Under this

S. Nageswaraiah
REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 Deemed-to-be-University Under Section 3 of the UGC ACT, 1956



ICFAI FOUNDATION FOR HIGHER EDUCATION

policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

(b) All computer software copyrights and terms of all software licenses will be followed by all employees of the institution.

(c) Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of the user/in charge of the section/dean of the Faculty to ensure these terms are followed.

(d) System Administrator is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and license agreements are adhered to.

(e) All software must be appropriately registered with the supplier.

(f) IFHE will be the registered owner of all software.

(g) All software installation is to be carried out by System Administrator

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

(i) Only software purchased in accordance with the software policy is to be used within the institution.

(j) Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

(k) All employees must receive training for all new software. This includes new employees, to be trained to use existing software appropriately. This will be the responsibility of System Administrator

(l) Employees are prohibited from bringing software from home and loading it onto the institution's computer hardware.

(m) Unless express approval from System Administrator is obtained, software cannot be taken home and loaded on a employees' home computer

(n) Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorization from the management is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the institution and must be recorded on the software register by System Administrator

(o) Un-authorized software is prohibited from being used in the institution. This includes the use of un-authorized duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses un-authorized copies of software will be referred to their respective Director/Dean for reprimand/counselling action. The illegal duplication of software or other copyrighted works is not condoned within this institution and Director of the College is authorized to undertake disciplinary action where such event occurs.

(p) Where there is a breach of this policy by an employee, that employee will be referred to Director of the respective College for reprimand/counselling action

(q) Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify system Administrator immediately. In the event that the breach is not reported and it is determined that

S. Jayalal

REGISTRAR

THE ICFAI FOUNDATION FOR HIGHER EDUCATION
(Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

an employee failed to report the breach, then that employee will be referred to the respective Director of the College.

24. Own Device Usage Policy

(i) At IFHE we acknowledge the importance of mobile technologies in improving institution communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to IFHE's network and equipment. This policy should be read and implemented in letter and spirit.

(ii) This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and I pads/Laptops etc for institution purposes. All staff who use or access IFHE's technology equipment and/or services are bound by the conditions of this Policy.

(iii) Personally owned mobile devices such as laptops, I pads, smart mobile phones are approved to be used by the individuals for institution/personal use.

(iv) Though the institution will not have any control over the applications installed in their respective devices, each individual is responsible for their own devices and the software installed in it. Any copyright infringements etc will be the sole responsibility of the individual.

(v) Employees when using personal devices for institution use will register the device with the relevant pass word for logging into the Wi-Fi network of the University.

(vi) System Administrator will have absolute right to provide or reject access to Wi-Fi facility to a user/device.

(vii) Personal mobile devices can only be used for accessing their e mails and personal whatsapp messages.

(viii) Each employee who utilizes personal mobile devices agrees:

(i) Not to download or transfer institution or personal sensitive information to the device. Sensitive information includes faculty/staff details/research projects/ e mail addresses intellectual property etc,

(ii) Not to use the registered mobile device as the sole repository for IFHE's information. All institution information stored on mobile devices should be backed up

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

(iv) Not to share the device with other individuals to protect the institution data access through the device

(v) To abide by IFHE's internet policy for appropriate use and access of internet sites etc.

(vi) To notify IFHE system Administrator immediately in the event of loss or theft of the registered device

(vii) Not to connect USB memory sticks from an untrusted or unknown source to IFHE's equipment.



ICFAI FOUNDATION FOR HIGHER EDUCATION

- (viii) All employees who have a registered personal mobile device for institution use acknowledge that the institution:
- (aa) Owns all intellectual property created on the device
 - (bb) Can access all data held on the device, including personal data
 - (cc) Will regularly back-up data held on the device
 - (dd) Will delete all data held on the device in the event of loss or theft of the device
 - (ee) Has first right to buy the device where the employee wants to sell the device
 - (ff) Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
 - (gg) Has the right to deregister the device for institution use at any time.

25. **Keeping Mobile Devices Secure**

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

- (ix) Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- (ii) Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
- (iii) Mobile devices should be carried as hand luggage when travelling by aircraft
- (iv) Any breach of this policy will be referred to System Administrator who will review the breach and determine adequate consequences, which can include referring the matter to the higher authority.

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

26. **Information Technology Security Policy (Penalties as per IT Act 2000 are given at Appendix 'A')**

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

S. Nagarajulu
REGISTRAR



ICFAI FOUNDATION FOR HIGHER EDUCATION

- (b) For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access control measures. No unauthorized entry into the server room is permitted. All the systems should be pass word protected and the switches should be physically protected under lock and key.
- (c) It will be the responsibility of System Administrator to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify the System Administrator immediately.
- (d) All security and safety of all portable technology, such as laptop, notepads, iPad, laptops etc. will be the responsibility of the employee who has been issued with these. Each employee is required to use locks, passwords, etc. to protect their devices and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.
- (e) In the event of loss or damage, system administrator will assess the security measures undertaken to determine if the employee will be required to reimburse the institution for the loss or damage
- (f) All devices such as laptop, notepads, iPads etc. when kept at the office desk is to be secured by relevant security measure here, such as keypad, lock etc.
- (g) All critical data to be backed up on daily basis, before closing hours of office.
- (h) It is the responsibility of the individual under whose charge the device is held to back up and store the backed up disk safely.
- (i) All technology that has internet access must have anti-virus software installed. It is the responsibility of System Administrator to install all anti-virus software and ensure that this software remains up to date on all technology used by the institution.
- (j) Robust fire wall to stall any malicious attacks on the system is the responsibility of the System administrator.
- (k) All information used within the institution is to adhere to the privacy laws and the institution's confidentiality requirements. Any employee breaching this will be dealt with under the provisions of this policy in conjunction with IT policy 2000.
- (l) Computers connected to Central's computer networks, whether owned personally or by the College, must be protected with up-to-date anti-virus software and must have the latest operating system security fixes installed.
- (m) Each individual is responsible for protecting his/her password for access to computer systems. Each user is responsible for all actions taken and uses of computer systems made under that individual's username.
- (n) Faculty, staff, students and guests must not tell others their passwords, post them in visible areas, or otherwise communicate a password to anyone other than IT Services personnel.
- (o) Users who have reason to believe that their password has been compromised must change it immediately.


REGISTRAR
THE ICFAI FOUNDATION FOR HIGHER EDUCATION
(Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

27. **Privacy and Confidentiality.** IFHE is committed to protecting the privacy of authorized users of its technology resources. Despite this intention, it cannot assure Faculty, staff and students that their uses of college computing and communications resources will be completely private. Information and messages sent over the Internet can be intercepted in various ways. Therefore, users of IFHE, IT technology with access to the Internet cannot assume that information they send over the Internet will be or remain confidential and inaccessible to anyone other than the intended recipient.

28. IFHE IT Cell routinely or without cause monitor an individual's network activity or electronic files. However, IT cell owns and maintains the computer and communication technology used by its students, faculty and staff, and has the right and responsibility to periodically access files to service and repair these systems and to ensure that college policies and applicable cyber laws are observed.

29. IT Services remotely manages college-owned computers from a centralized management console. This capability includes the ability to view computer screens remotely. Affected individuals will be given advance warning of such operations whenever possible.

30. IFHE will not access or monitor computer accounts, use of technology resources, or other electronic resources except when:

- (i) The user(s) authorizes such access
- (ii) The user has voluntarily made information accessible to the public by posting it to a web page
- (iii) It appears necessary to protect the integrity, security or functionality of University resources or to protect the IFHE from liability
- (iv) There is reasonable cause to believe that the user has violated or is violating this acceptable use policy or other University policies
- (v) An account appears to be engaged in unusual or excessive activity
- (vi) It is otherwise required by law

31. In general, information stored on computers is considered confidential, whether protected by the computer operating system or not, unless the owner intentionally makes that information available to other groups or individuals. IFHE will assume that computer users wish the information they store on campus local and shared computing resources to remain confidential. Similarly, privileged information on account usage (i.e., that available only to users with system privileges) will be held in confidence.

32. IFHE employees, and students working in campus offices, who because of their work have access to non-public (confidential) information about others must not disclose that information. Employees must protect from the view of visitors non-public information displayed on computer screens. Employees who access IFHE non-public information from off campus either through remote connection or by portable device,

[Signature]
 REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed-to-be-University Under Section 3 of the UGC Act, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

must take special precautions to ensure that information does not become accessible to others and that devices are not lost or stolen.

33. When college computers are discarded, system administrator will completely erase all data and software from local storage drives before the computer leaves campus. If the computer is to be reused, IT Services may reinstall operating system software consistent with applicable license agreements.

34. Requests for disclosure of confidential information will be reviewed by the administrator of the information system involved. Such requests will be honored only when approved by Management or Director of the respective College when required by law enforcement agencies.

35. **Technology Access**

(a) Every employee will be issued with a unique identification code to access the institution technology and will be required to set a password for access every facility.

(b) Each password is to be complicated enough not to breach and is not to be shared with any employee within the institution.

(c) System Administrator is responsible for the issuing of the identification code and initial password for all employees.

(d) Where an employee forgets the password or is 'locked out' after three attempts, then System Administrator is authorized to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

(e) Employees are only authorized to use institution computers for personal use in extraordinary circumstances, that to on approval from the Director of the College or the Registrar of the University.

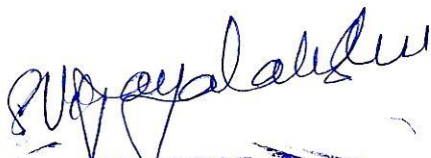
36. **Information Technology Administration Policy**

(a) This policy provides guidelines for the administration of information technology assets and resources within the institution.

(b) All software installed and the license information must be entered in a register held with System Administrator. The register must record the following information:

- (i) What software has been procured
- (ii) What license agreements are in place for procured software package
- (iii) Renewal dates if applicable.

(c) System Administrator is responsible for the maintenance and management of all service agreements for the institution technology. Any service requirements must first be approved by System Administrator.


REGISTRAR
THE ICFAI FOUNDATION FOR HIGHER EDUCATION
(Deemed-to-be-University Under Section 3 of the UGC Act, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

- (d) System Administrator is responsible for maintaining adequate technology spare parts and other requirements, such as toners, printing paper and other computer related accessories and spares.
- (e) A technology audit is to be conducted by a team detailed by the Management annually to ensure that all information technology policies are being adhered to.
- (f) Use of technology to download, store or distribute pirated materials will lead to disciplinary action against the individual.

PART -II**IFHE – WEBSITE POLICY**

37. **The Website** The ICFAI Foundation for Higher Education, Hyderabad (IFHE), (Deemed-to-be-University) home page (<https://www.ifheindia.org>) is the official domain name for the University. The "official" home page structure includes the home page, the sub-domains/department/school sites, internal link pages, and other sites/links integrated into the home page structure. The site is hosted on a cloud server with third party.

38. **Purpose of Website** The objective of the home page is to provide a point of entry on World Wide Web for the Prospective students, Students, Faculty & Staff, Employers and general public to the University's officially recognized information sources that include program information, teaching & learning, research & publications, seminars & workshops, marketing and the administration. Information is provided by the Office of the Dean/Director/Registrar, IT Services, various administrative and academic units, faculty, staff, and students. The websites' purposes are to enhance communication and learning, and to help inform decision-making by providing current information, and links to news and events of general interest.

There are two main sections to the website: -

- (a) The front end published site, which is open to all (<https://www.ifheindia.org>).
 - (b) The private back-end site, which is available only to authorized faculty/staff/employees of the university and controlled by User Id and Password.
39. User accounts are only created with the approval of the concerned Manager/Department Head/Dean/Director/Registrar.

40. **Access, Approval and Publishing** Content on the university website is controlled by role access. There are 3 roles: Indenting Department (School/Faculty), Approving Authority and Publishing on the website.

- (a) Initially, all content to be uploaded on the website must be reviewed by the Content Author or Editor/Faculty/a designated senior person of the Department.
- (b) It will be approved by the Competent Authority like Dean/Director before going live.
- (c) The content/material so approved by the Competent Authority is sent by the Department to the IFHE University Web Team. The University web team in

ICFAI FOUNDATION FOR HIGHER EDUCATION

turn process and forward it to CIT Web Team in standard format with workflows and detailed information/instructions if any.

(d) CIT Web Team will evaluate the information so received, will ensure that standards are met and publish/update/upload it to the site unless expressly authorized by the Department Head.

41. **Website Updation and Maintenance** The IFHE Website is the public entry point for many to the University. The University Webmaster continually designs & develops, upgrades, and reviews the University Web site, taking into account latest design patterns and trends, introducing new technologies and evaluating methods of access in providing up-to-date, accurate information methodically and attractively.

(a) The web pages are regularly reviewed for accuracy and updated as required. It must be current, accurate and consistent. This review is occurring at least half-yearly. It is the responsibility of Head of the concerned department (school/faculty) to ensure this happens and their School/Faculty site is up-to-date and accurate.

(b) Department/School/Faculty wishing to post announcements on the home page or other portions of the website should submit their request through official email or letter to the CIT Web Team routed thru University Web Team.

(c) Photographs on the main site are changed on a regular basis by the Website Administrator as provided by the Department(s).

(d) Faculty Pages are created in concerned department web link. They may provide their latest Bio-Data and photo for a web link.

(e) During the process of review if any "Under Construction" pages are identified pertaining to a School/Faculty, the Dean/Director is requested thru email to provide such information within stipulated time. Otherwise, such pages will be taken down after a week.

(f) Basic branding guidelines must be followed on website to ensure a consistent and cohesive image for the University.

42. **Required Style Specifications** All pages on the main IFHE website must comply with the following style specifications:

(a) The website is designed for best case viewing on multiple platforms, newer versions of Google Chrome, Firefox Mozilla, Internet Explorer, Opera and Netscape, etc.

(b) The look and feel, color scheme, and fonts of the Web pages may vary slightly according to user's monitor's setting.

(c) Mobile viewing of the website is also optimized for all major smart phones.

(d) Files for download must be under 20 MB in size.

(e) In case of audio and video, the quality must be reasonably good. Video which is inappropriate in content, blurry, unsteady, or difficult to view will not be uploaded. Audio that is difficult to hear or inappropriate in content will not be posted. In order to be useful and convenient to the user, all files posted must be under 20 MB in size and 10 minutes in length.

(f) To enable faster downloading, scanned photographs should be limited to 144 dpi.

ICFAI FOUNDATION FOR HIGHER EDUCATION

(g) Links to pages that are defunct or "under construction" should not be created or should be removed.

43. **Privacy Policy** IFHE is committed to respecting privacy. Personal data privacy is a new and evolving area, and the Society is evolving to meet these demands. The following privacy policy is implemented:

- (a) Personal contact information of students including residential/correspondence address, e-mail id, phone number, and other information that could be used by unauthorized individuals, will not be published on any IFHE website.
- (b) Video or audio files posted on any IFHE website must adhere to Website Policy. Proper written permission from those who have been audio- and / or video-recorded must be obtained by the person or persons doing the recording.
- (c) Links to external websites will be checked thoroughly before inclusion on the university website. The sites will be checked for the suitability of their content for their intended audience, and meet the standards of IFHE.
- (d) All written work will be reviewed by the concerned department/school/faculty to ensure that it is in no way defamatory.
- (e) Written work will be checked by the concerned department/school/faculty to ensure that no copyright or intellectual property rights are infringed.
- (f) All written material will be checked for its suitability for its intended audience.
- (g) IFHE does not sell or distribute any information obtained from our visitors to a third party, under any circumstance.

44. **Advertising** Unless approved by the Competent Authority, the advertising or direct sale of non-University related products and services is prohibited on all sections of the IFHE Web site or its sub-domains.

45. **Logos, Trademarks, and Graphics of Website** Official website of the IFHE University has its own logo, seal, and graphics relating to the University that may be subject to agreements and any use of these would require prior approval of competent authority. Any unauthorized use of the content and proprietary logos, service marks, and trademarks may violate copyright laws, trademark laws, the laws of privacy and publicity and certain civil and criminal statutes.

46. **Refund / Cancellation Policy for Online Transactions through Website** Prospective students/Students make payments online on the IFHE Website using secure Internet Payment Gateway for availing various services. In the event that any payment is to be refunded The IFHE University will endeavor to make the refund payment back to the credit card/debit card/ internet banking account from which the original payment was made. If for any reason the payment cannot be made to the originating card/account for reasons beyond the IFHE's control a cheque refund will be made to the card/account holder. In the event of a student withdrawing him/herself from a program of study, he/she must approach the Program Co-coordinator/Student Services department in writing to this effect. Entitlement to a refund of tuition fees will be determined as specified in the Handbook of Student Regulations.

Shraddha
REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



47. **Website and Web Server Security** The website visitor may not use any device, software or routine, including but not limited to any viruses, Trojan horses, worms, time bombs, denial-of-service attacks, other malicious code or repeated "hacks" or "attacks" on the Web server hosting IFHE website, intended to damage or interfere with the proper working of the Site or to surreptitiously intercept or expropriate any system, data or personal information from the Site. You may not take any action, which imposes an unreasonable or disproportionately large load on the Site's infrastructure, including but not limited to denial of service attacks, "spam" or any other such unsolicited overload technique. Violators or Cyber attackers or Hackers will be prosecuted to the maximum extent permissible by law under Indian Information Act 2000 and the I.T Amendment Act 2008.

48. **Responsibility of Website Management** The University's Web site is maintained by Head, Central Web Team and Staff of Central Web Team.

- (a) The Team maintains a Register to record:
 - (i) List of domain names registered in the name of University
 - (ii) Dates of renewal for domain name(s)
 - (iii) Details of hosting service provider
 - (iv) Expiry dates of hosting services
 - (v) Updates wherever and whenever carried out
- (b) Content on the University website is to be accurate, appropriate and current.
- (c) Content on the website must follow the laid down policy on the subject.
 - (i) The content of the website is to be reviewed every week/month
 - (ii) The following persons are authorized to make changes to the institution website: Senior Web Designer/Web Designer
 - (iii) Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the University.
 - (iv) All data collected from the website is to adhere to the Privacy Act
 - (v) At least two Web Designers and Programmer cum Database administrator, who have the sufficient technical knowledge and expertise maintain and edit the website, with sufficient access rights and supervised by Team Lead/Head, CIT Web Team. At the end of a term of office of any Team member, knowledge transfer happens to a successor.
 - (vi) Website Disruption : In the event that University website is down/inaccessible, the following actions must be immediately undertaken
 - (aa) Head/Team Lead, Central Web Team must be notified immediately.
 - (bb) Website host to be notified thru e-Mail or SMS or thru direct contact over phone
 - (cc) Initiate any emergency actions if required

49. **Jurisdiction** The IFHE Website is in the public domain and information uploaded on the website is subject to official certification as per Information

[Signature]
 REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

Technology Act. All information that is mandatory by different monitoring agencies is changed with the changed requirements of the agency concerned. For any interpretation regarding information hosted on our website, the decision of Vice-chancellor is final and the legal jurisdiction is limited to Hyderabad, Telangana, India only.

50. The IFHE website provide Internet access to college information resources and external information sources that support teaching, learning, marketing and the administration of the college. Information is provided by the Office of College Relations, IT Services, the Library, various administrative and academic units, faculty, staff, and students. The websites' purposes are to enhance communication and learning and to help inform decision-making by providing current information.

Online fee Collections/Payments

51. ICFAI University has recognized the electronic banking ever since the University started its academic activity in the Campus at Shankerpally. Towards this, the university got installed the ATM machines of HDFC Bank and State Bank of India, ATM being the extensively used electronic banking service. It is a beginning of electronic banking in the University. The development of electronic banking under different modes has been expedited by RBI and Government of India by enactment of IT Act 2000 to safeguard the interest of all the people involved and the University is a follower of the new systems to the benefit of the students.

52. In view of the enormous advantages in fee collections and payment solutions available in e-banking, the University introduced online fee collections. Towards this, the IT department of the University developed program wise platforms/websites/screens and got integrated with the payment solution systems of a Bank especially ICICI Bank. Eventually, eazy-pay payment solutions of ICICI Bank are put in place for fee payment by the students. Eazy-pay is a single platform for multiple collection modes which facilitates single Management Information System (MIS) reconciliation for all collection modes. The students can make fee payments through NEFT/RTGS/IMPS/Credit Card/Debit Card/Internet Banking sitting at home/working at their desk. The systems are foolproof and secure.

53. The University also has got installed PoS machines in the University to facilitate payment of petty amounts by the students.

54. With regard to payments by the University, the University has online payment systems and tie up arrangements with different banks. Primarily the University has online payment system of all statutory payments. The other payments to vendors/service providers, the university makes payment through NEFT/RTGS/ Bank upload printed cheques.

55. In a nutshell, the University is experiencing the advantages of e-banking and going forward the University will introduce other new systems to go hand in hand with the systems of the RBI/Government of India.

[Signature]
REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



PART –III**EMERGENCY MANAGEMENT : INFORMATION TECHNOLOGY**

56. The following procedure will be adopted to reduce the down-time of the hardware:-

- (a) This policy provides guidelines for emergency management of all information technology within the institution.
- (b) Where there is failure of any of the institution's hardware, this must be referred to System Administrator immediately.
- (c) It is the responsibility of System Administrator to do the trouble shooting in the event of IT hardware failure.
- (d) It is the responsibility of System Administrator and his team to undertake tests on planned emergency procedures once in six months to ensure that all planned emergency procedures are appropriate and minimize disruption to institution operations.

57. **Virus or other security breach**

- (a) In the event that the institution's information technology is compromised by software virus or Trojan or cyber-attack such breaches are to be reported to System Administrator and Director of the respective college immediately.
- (b) System Administrator is responsible for ensuring that any security breach is dealt with within a reasonable time frame to minimize disruption to institution operations.

58. **Academic Integrity**

- (a) The University expects Faculty/staff/ students to conduct themselves with integrity, in ways which honor community, exemplify fairness, demonstrate respect and accept responsibility. The basic approach to maintaining this code of conduct is self-discipline.
- (b) These rules apply to all Faculty/staff and students. Anybody found to have committed the misconduct is subject to sanctions. All should exemplify honesty, integrity and a respect for truth in all of their dealings. Behavior that demonstrates a lapse of integrity includes, but is not limited to:

- (i) Knowingly furnishing false, falsified, or forged information to any member of the college community, such as lying to a college employee, falsification or misuse of documents, accounts, records, identification or financial instruments;
- (ii) Unauthorized possession, duplication, or use of means of access to software being used in the University;
- (iii) Action or inaction by someone in collusion with a wrongdoer which fails to discourage a known and obvious violation of college policy or law;

Signature
 REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

- (iv) Violations of positions of trust or authority within the IFHE community;
- (v) Tampering with the network system/hardware/software with the malafide intention of breaking down the existing system.
- (vi) Email harassment; spamming; chain letters; hoaxes; falsifying mail headers
- (vii) Use of technology to intentionally access, create, store or transmit pornographic materials
- (viii) Accessing violence-oriented or harassment-oriented websites unless such information is being used for an academic class
- (ix) Damaging any system by introducing computer viruses, worms, or spyware
- (x) Unauthorized attempts to alter data files or systems
- (xi) Disrupting or degrading the performance of computer, network, website, or e-mail systems
- (xii) Any action compromising or attempting to compromise the integrity or security of computer systems or networks, whether internal or external to campus
- (xiii) Sharing or revealing individual or organizational authorizations and passwords
- (xiv) Unauthorized access to email, voice mail, or other communications intended for others
- (xv) Use of technology resources to impersonate another individual or entity
- (xvi) Unauthorized use of technology to access non-public (confidential) information
- (xvii) Intentional damaging, disabling, or removal of software or hardware
- (xviii) Use of technology resources for commercial purposes or personal financial gain
- (xix) Implying in any way that IFHE is directly involved in political campaigns or campaign fundraising
- (xx) Any other activity that violates Cyber laws, or IFHE policies

59. **E mail.** E-mail at IFHE is a service provided to enhance communication regarding teaching, learning and the general operations of the college. E-mail accounts are available to every student, staff, and faculty member of the college. All are required to have an IFHE e-mail account and to check it regularly. Some of the important guidelines for e mail usage are as follows:-

- (c) The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- (d) Using the facility for illegal/commercial purposes is a direct violation of the university's IT 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

Sudhakar
 REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 Deemed-to-be-University Under Section 3 of the UGC Act, 1956



ICFAI FOUNDATION FOR HIGHER EDUCATION

software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

(e) While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

(f) User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.

(g) User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.

(h) Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.

(i) User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

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

(k) While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

60. The official mass email service is restricted to those messages that meet one or more of the following standards:

(a) Provides essential information for the operation or execution of daily business;

(b) Notifies the campus community of significant events or changes in governance, policy, and practice;

(c) Alerts the campus community to situations around health and safety, as on required basis from the Administration; or

(d) Communicates important information from the Management.



REGISTRAR

THE ICFAI FOUNDATION FOR HIGHER EDUCATION
(Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

- (e) Mass emails that do not meet these requirements of urgency and/or critical information should seek other methods.
- (f) Messages may be posted to the Students list only by those having special permission

Un acceptable E mail Usage

61. The following uses of e-mail are considered inappropriate and unacceptable by IFHE, Hyderabad:

- (a) Harassing or hate mail; any mail sent to individuals that is abusive, threatening, or discriminatory toward others
- (b) Initiating or retransmitting viruses, worms, virus hoaxes or any harmful software
- (c) Chain mail that misuses or disrupts resources; E-mail sent repeatedly from user to user, with requests to send to others.
- (d) Sending large quantities of email to an individual's mailbox (e.g., email "spamming") which has the effect of interfering with or causing impairment to that individual's activities
- (e) Posting or sending personal, sensitive or confidential information about another person, including medical information about an employee or student, via any form of electronic communication
- (f) False identification; any messages that misrepresent or fail to accurately identify the true originator
- (g) Any message that violates a policy of the College.
- (h) Messages posted to the Employees list or to any of its sub-lists should be of general professional interest to the members of that list or sub-list.
- (i) Personal advertisements and discussion oriented postings are not appropriate for mass distribution via the Employee list or any of its sub-lists.

Cyber /Copyright Law adherence

62. College students, faculty and staff must be familiar with and adhere to current Cyber/copyright Laws. The ease with which original works can be copied and transmitted anywhere in the world has led to greater need to understand these laws.

63. Copyright is of great importance to us as we pursue our educational mission. It is in our interest to protect the intellectual property that we may create and to exercise "fair use" of copyrighted works that we may be using in our research, teaching and learning. As an educational community, we realize that all educational use may not be "fair use." We must be prepared to ask for permission to copy when statutory exemptions do not apply, to pay copyright fees, to use existing licenses or to purchase additional licenses or copies of works in order to comply with copyright.


REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



64. Copyright protects a wide range of resources including, but not limited to: books, articles, photographs, paintings, sculptures, architectural works, dramas, music, sound recordings, ballets, motion pictures and other audio-visuals, software, and websites.

65. A copyright infringement may occur when someone other than the copyright owner exercises any of these exclusive rights. Possible infringements include photocopying, uploading to websites, sharing files, copying software, public film exhibitions, and music performances. Creating web pages for educational and research purposes, digitizing and transmitting works for courses, or producing e-portfolios are examples of activities that may involve incorporation of copyrighted works and are governed by copyright law.

Responsibilities of IT Cell in IFHE

66. Duties and responsibilities of IT cell headed by System Administrator are as follows:-

- (a) Maintenance of the Computer net working in the IFHE campus.
- (b) Monitor the work of AMC vendors.
- (c) Allotment of e mail addresses to new faculty, staff and students
- (d) Attend to service calls by the Faculty, staff and Students.
- (e) Provide un interrupted Wi-Fi facility to the entire campus and maintaining 1 GB Wi-Fi speed.
- (f) Ensure the IT resources are not misused by the Faculty, staff and students.
- (g) Preparation of gate passes for the IT equipment, where there is a requirement to carryout repairs to these systems at the location of the vendor.
- (h) Attend to all the emergency calls for service interruptions.
- (i) Ensure serviceability of all the Computers, peripherals and net working system.
- (j) Look out for constant up gradation of software and hard ware.
- (k) Advice suitably regarding up gradation of Networking systems, Servers, Computer systems and peripherals.
- (l) Monitor net work usage and plug excess usage by an individual, if need be, identify the IP address and block it.
- (m) Monitor and block unwanted malicious web sites. Deny access to prohibited sites.
- (n) Monitor the firewall performance and upgrade periodically.
- (o) Ensure the servers and the Computer systems are updated with latest versions of software.
- (p) Plug loopholes in the security software.
- (q) Install and monitor antivirus software in all the systems.
- (r) Ensure the connectivity of LAN net work.
- (s) Plan for further expansion of network


REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)



ICFAI FOUNDATION FOR HIGHER EDUCATION

- (t) As system Administrator, during random check if any faculty ,staff or student misusing the Wi-Fi connection and indulging in surfing of net for pornography, child pornography, the same should be brought to the notice of Director of the respective college and the Management.
- (u) IT Cell is the campus network backbone such that service levels are maintained as required by the University Sections, departments, and divisions served by the campus network .
- (v) System Administrator will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
- (w) It is not the policy of the University to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the University's Internet links.
- (x) Major network expansion is also the responsibility of the IT Cell of IFHE, every 3 to 5 years,
- (y) IT cell will review the existing networking facilities, and need for possible expansion. Network expansion will be carried out by IT Cell when the university makes the necessary funds available.
- (z) IT cell is authorized to restrict network access to the Sections, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions. Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.
- (aa) E waste will be disposed off as per Telangana Government E waste Management policy of 2017

Summary

67. The "Deemed to be" University IT policy has been made to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus. This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information. It is our collective responsibility to protect and avoid misuse of the IT resources in the Campus.


REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed to be University Under Section 3 of the UGC ACT, 1956)



Offences**Appx A**

(refers to para 26 of IT Policy)

List of offences and the corresponding penalties under IT Act 2000

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to Rs 200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to Rs500,000
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to Rs100,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to Rs100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹100,000



S. Jayaraman
REGISTRAR
 THE ICFAI FOUNDATION FOR HIGHER EDUCATION
 (Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)

66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyber terrorism	If a person denies access to an authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyber terrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.

S. V. Jayalakshmi



REGISTRAR
THE ICFAI FOUNDATION FOR HIGHER EDUCATION
(Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)

ICFAI FOUNDATION FOR HIGHER EDUCATION

68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to 2 years, or/and with fine up to ₹100,000
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to 2 years, or/and with fine up to ₹100,000



S. V. Jayalalitha

REGISTRAR

THE ICFAI FOUNDATION FOR HIGHER EDUCATION
(Deemed-to-be-University Under Section 3 of the UGC ACT, 1956)