# INDIAN INSTITUTE OF INFORMATION TECHNOLOGY UNA

# DRAFT ICT INFRASTUCTURE POLICY

# Table of Content

# 1. Introduction

Indian Institute of Information Technology Una (IIITU) is one of the youngest and fastest growing Institutes of National Importance established by an Act of Parliament for imparting higher education to cater to the growing needs of the industries. Besides, it conducts basic and applied research with over 35 faculty members, 800 students, and 500 alumni. The Institute offers five BTech programs each in CSE, CSE (Data Science) CSE (Cyber Security), ECE, and IT disciplines, MTech program in CSE with specialization in Cyber Security/Data Analytics, and PhD programs in School of Computing, School of Electronics, and School of Basic Sciences. IIITU is continuously collaborating with the industry to expand research and bring the technology to the use of the masses. It is engaged in a wide range of industrially relevant activities including training graduate and undergraduate students for the industry, conducting research in cutting-edge areas, consulting, and advising the industry as well as engaging in socially relevant activities to benefit society at a large.

The institute has state of the art Information and Communication Technology (ICT) infrastructure in place, to support its academic and research activities. The institute has created an ICT Cell for the smooth functioning of ICT related activities, development and maintenance of ICT infrastructure. The major components under ICT Cell are as follows:

a) Computing Machines (Desktop, Laptop, etc) and Peripheral Devices.
b) Network Infrastructure.
c) Video Surveillance Infrastructure.
d) Website/ERP/Other similar portals.
e) Biometric Attendance System.
f) Server/Cloud Infrastructure/Services
g) Network/Internet Based Services/Intranet Services

The role of ICT Cell is to provide the technical support for all the above mentioned components. The ICT Cell will address hardware-related problems and legally purchased software issues. The cell will be responsible only for solving the hardware related problems or Operating Systems (OS) or any other application software that were legally purchased by the Institute. Other key responsibilities of the ICT Cell are as follows:

i. **Maintenance:** The ICT Cell is responsible for maintaining all IT related equipment owned by the institute under warranty or maintenance contracts period. Any addition/deletion/modification in any service/infrastructure shall be conducted or initiated by the cell upon a written request by the respective organizational unit with the approval of the competent authority.
ii. **Handling of Complaints:** The ICT Cell will handle complaints about network-related problems and hardware issues within a reasonable time.
iii. **Use of Authorized Software**: The ICT Cell will not install unauthorized software on Institute systems.

iv. **Policy Violation Reporting:** The ICT Cell will report the competent authority about incidents that violate Institute ICT policies.

v. **System Rebuild:** Rebuilding computer systems must adhere to Institute guidelines to ensure proper functionality and security. When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net. Further, before reformatting the hard disk, dump of only the data files should be taken for restoring it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

For a smooth functioning/management/maintenance of IT infrastructure, this policy is framed with following purpose and scope:

***Purpose***

This policy aims to establish guidelines for the acceptable use of ICT equipment/components/services at IIIT Una to protect both users and the institute from potential risks, including virus attacks, network compromise, legal issues, etc.

***Scope***

The policy applies to students, employees, contractors, consultants, and other personnel associated with IIIT Una and third-party affiliates. It encompasses all equipment/components/services owned or leased by institute, as well as privately owned devices connected to institute's network. The Students, Teaching and Non - Teaching Staff, Management and visiting Guests and Research Fellowship Members of IIITU availing computing, networking, and IT facilities are expected to abide by the following rules, which are intended to preserve the utility and flexibility of the system and protect the privacy and work of students and faculty. Failure to agree with any provision necessitates informing the system administrators at the ICT Cell and discontinuing the use of any provided access facilities until resolution.

## 2. General Rules

i. **Authorized Use:** Students, Teaching and Non-Teaching Staff, Management, Visiting Guests, and Research Scholars are authorized to use computing, networking, and other IT facilities for academic purposes, official Institute business, and personal purposes, provided such use does not violate any law or Institute policy.

ii. **Unauthorized Access:** Users are prohibited from gaining or enabling unauthorized access to restricted IT resources on the Institute network.

Violations may lead to disciplinary action, and could also incur civil and criminal liability under national and international cyber laws, including the Information Technology Act of India. However, the institute reserves all the rights to access and analyze the IT resource and Information for any legal and/ or institutionally provisioned operation, on its own.

iii. **Inappropriate Content:** Users are prohibited from sending, viewing, or downloading fraudulent, harassing, obscene (i.e., pornographic), threatening, or otherwise inappropriate messages or materials that violate applicable law or Institute policy. Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful e.g. when such content is received through email etc. As a generalised policy any contribution towards the destruction or distortion of congenial academic or work environment is prohibited.

iv. **Intellectual Property**: Users must respect intellectual property rights and copyright laws. Unauthorized sharing, use, or distribution of copyrighted materials, illegal or pirated or unlicensed software on the Institute's IT resources is strictly prohibited.

v. **Open Source Recommendations**: The Institute recommends using Open Source OS and Processing Software (PS) such as Ubuntu/CentOS and LibreOffice/OpenOffice/WPS Office. Users are encouraged to migrate to these recommended systems unless a valid technical limitation is presented. In case of technical limitations in such adaptation, relaxation may be requested in written from competent authority on valid grounds.

vi. **Data Privacy and Security**: Users must respect the privacy of others and are prohibited from attempting to access or disclose information without proper authorization. The broader concept of data privacy must be honoured by each user.

vii. **Data Integrity**: Users must not attempt to vandalize, damage, or alter any data inappropriately, whether by accident or deliberately. The integrity of information resources must be preserved by all users. Any interference, disruption or encroachment in the institute ICT resources shall be a clear violation of the institute policy.

viii. **Resource Availability:** Users should not intentionally or unintentionally disrupt the availability of ICT resources.

ix. **Department Policies**: Individual schools, hostels, and units may implement additional conditions of use for ICT resources under their control, provided these conditions are consistent with the Institute's IT policy. It will be the responsibility of the respective organisational units to publicize and enforce such conditions of use. In cases where use of external networks is involved, suitable policies can be practiced in compliance with the broad prerogatives of policies of the institute.

x. **Legal Compliance**: The Institute may be required to provide IT information, resources, and records to third parties as part of legal investigations or monitoring. Users should expect only a reasonable expectation of privacy on Institute IT resources.

xi. **Equipment Care**: Users are expected to take proper care of equipment and report any malfunctions to the appropriate staff. Moving, repairing, reconfiguring, modifying, or attaching external devices to the systems should not be attempted by the users. Any action (intentional or unintentional) causing damage to ICT infrastructure shall be treated as misconduct and strict disciplinary action will be taken.

xii. **Laboratory Conduct:** Food or drink is not permitted in laboratories. Activities that create noise or disruption are also prohibited.

xiii. **Policy Violations:** Violations of this policy will be treated as academic misconduct, misdemeanours, or indiscipline, and appropriate actions will be taken by Institute authorities.

xiv. **Policy Updates:** The policy may be updated as needed, with new policies taking effect immediately after an announcement via institute website or email or printed notices or news groups.

xv. **Monitoring and Surveillance:** With the approval of the competent authority, authorized individuals within institute may monitor equipment, systems, and network traffic for legal, security, and maintenance purposes. *IIIT Una reserves the right to conduct periodic audits of networks and systems to ensure compliance with the policy.* The institute may seek services from the third party service providers.

## 3. Email Account Use Policy

The employee/students of the institute are eligible to have institute official domain id (@iiitu.ac.in). The user may contact the ICT Cell administrator by submitting an application in a prescribed proforma available on institute website to create the email on institute domain. The general rules for institute email uses are as follows:

i. **Email account creation:** Only one email account will be created for a user. An email account once created should not be repeated for any new user.

ii. **Email account transfer:** Various email IDs for administrative position holders are fixed and will be transferred to the respective person at the time of charge handover.

iii. **Email account suspension:** If a student is suspended for some duration due to a disciplinary action, the Email ID of the student will also be suspended for the same duration.

iv. **Email account deletion:** The Email IDs of the students will be automatically deleted after a period of two months from the date of the last exam of the final semester. If a student is terminated or leaves the institute in between, the Email ID of the student will be deleted after two months from the last date at institute. As per New Education Policy 2020, if a student rejoins the institute after taking a break, (s)he will be treated as a fresh entrant and new Email ID will be created. The Email IDs of the employees will be deleted after serving the notice period. However, under some exceptional cases (for example, awaiting the response from a Journal regarding the decision on a research paper submission, etc.), the deletion may be prolonged for a duration decided by the competent authority after receiving a written request from the user. The users are advised to back up the data and initiate the automatic email forwarding service to their personal email IDs to avoid loss of data/information. If an employee retires from the institute, (s)he will retain the Email ID for life.

v. **Formal Communications**: Institute email services should be used for formal Institute communication and academic and official purposes.

vi. **Prohibited Use:** Using Institute email for illegal or commercial purposes is a violation of Institute policy and may lead to strict disciplinary action. The illegal use included, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk email messages, and generation of threatening, abusive, obscene or fraudulent messages/images. Users should refrain from forwarding messages from institute domain (@iiitu.ac.in)/network to external parties without explicit consent. Harassment via email, telephone, or paging is strictly prohibited. Sending unsolicited email messages, including spam, is not permitted. Unauthorized use or falsification of email header information is prohibited. Solicitation of email for purposes other than personal use is not allowed. Creating or forwarding chain letters or pyramid schemes via email is prohibited.

vii. **Attachments:** While sending large attachments to others, user should make sure that the recipient has email facility that allows the recipient to receive such large attachments.

viii. **Mailbox Management:** The users should maintain their mailbox usage below 80% to avoid mail bounce issues.

ix. **Security Awareness:** Users should be cautious about opening emails or attachments from unknown or suspicious sources. Even the emails with suspicious or dubious looking attachments from a known source must be opened after confirming the authenticity from the sender.

x. **Backup and Configuration:** Users should configure their email software to regularly download emails and back up their emails to avoid server overload. It is user’s responsibility to keep a backup of the incoming and outgoing mails of their account.

xi. **Account Sharing:** Sharing email accounts is prohibited. Each user is responsible for any misuse of their email account.

xii. **Privacy:** Attempting to intercept or access other’s email accounts is prohibited.

xiii. **Shared Computers:** Users should log out of email accounts on shared computers. 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.

xiv. **Impersonation:** Impersonating another person's email account is a serious offense.

xv. **Responsibility:** Users are responsible for ensuring their email account adheres to the Institute's usage policies.

The ICT Cell shall not be held responsible for any loss of the data/service due to any reason.

## 4. Social Media Policy

This policy provides guidance for the use of social media, which should be broadly understood for purposes of this policy to include WhatsApp, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others. The users should adhere to the following guidelines when using social media in reference to the institute:

i. **Impact Awareness:** The users should be aware that their social media activity can affect their personal and the Institute's image. The users are thus advised to act wisely while using social media platforms.

ii. **Content Observation:** The ICT Cell may monitor social media content related to the institute. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to the Institute, its employees, or students or alumni.

iii. **Prohibited Content:** Posting defamatory, pornographic, proprietary, harassing, or otherwise inappropriate content that can create a hostile work environment or which may hurt religious and sentiments of any one or any Community, is prohibited.

iv. **Confidential Information**: The users should not post confidential or non-public information. If there are questions about what is considered confidential, the users should check with the competent authority.

v. **Press and Legal Inquiries:** Media and legal inquiries related to social media must be referred to competent authority.

vi. **Antagonistic Situations:** The users should seek advice from the competent authority, if a social media situation threatens to become antagonistic.

vii. **Permission for References:** The users should obtain permission before referring to or posting images of others. Additionally, users should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.

viii. **Work Responsibilities:** Social media use should not interfere with user’s responsibilities at the Institute. The Institute’s computer systems are to be used for official purposes only. When using Institute’s computer systems, use of social media for business purposes is allowed only to those whose work profile requires use of social media (ex: Facebook, X (Formerly Twitter), Institute blogs, LinkedIn, WhatsApp, Instagram, etc.). Personal use of social media during work/study hours (as per time table) is discouraged and may result in disciplinary action. Subject to applicable law, online activity after work/study hours that violates Institute’s policy may subject to disciplinary action against the user.

ix. **Separate Accounts:** Users are encouraged to keep Institute related social media accounts separate from personal accounts.

## 5. Biometric Policy

Biometric Information means personal information stored by the institute about an individual's physical characteristics that can be used to identify that person. Biometric Information can include, but is not limited to: fingerprints; voice patterns; face, hand, retina or ear features; and other biological traits that can be used to identify an individual.

- The institute will not sell, lease, trade, or otherwise profit from an individual's Biometric Information.
- Biometric Information will not be disclosed by the institute unless (a) consent is obtained, or (b) disclosure is required by law, including required disclosure to law enforcement authorities. This Policy is not intended to restrict communications or actions protected or required by law.
- The institute will destroy biometric data when the initial purpose for obtaining or collecting such data has been fulfilled or immediately after serving the notice period, whichever occurs first.

## 6. Video Surveillance Policy

ICT Cell will provide the necessary infrastructure and maintenance services for video surveillance of the institute premises. The Estate/Security office will be responsible for the monitoring and handling of the same.

i. **System Components:** The surveillance system includes cameras, monitors, multiplexers, recorders, storage devices, etc.

ii. **Camera Placement:** Cameras are strategically located, with no hidden cameras, and signage is used to inform about surveillance. Cameras focusing on the frontages or rear areas of private accommodation are discouraged.

iii. **Purpose:** The primary purpose of the surveillance system is to reduce crime and ensure safety. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

iv. **Control Room Access:** Images/Videos captured by the system will be monitored and recorded in the Security Control Room, "CCTV room", twenty-four hours a day throughout the whole year. The Estate/Security office will deal with the handling/supervision of the Control room by creation and implementation of the appropriate policy as per applicable laws. In addition, the following should be considered:

- No unauthorised access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, police officers and any other person with statutory powers of entry.
- Staff, students and visitors may be granted access to the Control Room on a case- by-case basis and only then on written authorisation from the Competent Authority. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Control Room.

- Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organisation they represent, the person who granted authorisation and the times of entry to and exit from the centre. A similar log of the staff on duty in the Security Control Room and any visitors granted emergency access will be kept.
- Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.
- Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.
- All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

v. **Recording Retention**: The infrastructure will be provided for retention of the recordings for a limited time as per the requirements of the Estate/Security office.

- Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.
- Images will normally be retained for limited period from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.
- All hard drives and recorders shall remain the property of Institute until disposal and destruction.

vi. **Access to Images:** Access to surveillance images is strictly controlled and logged by the Estate/Security office as per following:

- All access to images will be recorded in the Access Log as specified in the Procedures Manual.
- Access to images will be restricted to those staff who need to have access in accordance with the purposes of the system.
- Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

a) Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder.

b) Prosecution agencies .

c) Relevant legal representatives.

d) The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime.

e) People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.

f) Emergency services in connection with the investigation of an accident.

- CCTV/IP Camera digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by CCTV/IP Camera is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.
- A person whose image has been recorded and retained and who wishes access to the data must apply to the competent authority in writing along with applicable fees. Subject to the availability, a copy of the data will be arranged and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. A response will be provided promptly and in any event within forty days of receiving the required fee and information.
- The Data Protection Act gives the competent authority the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
- All such requests will be referred to the Security Control room Supervisor by the competent authority.
- If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

vii. **Processing Prevention Requests:** An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual. All such requests should be addressed in the first instance to the competent authority, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

viii. **Complaints:** It is recognised that members of Institute and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security/Estate Head.

## 7. Guidelines for the ICT users

Following guidelines will be applicable to all users using the Institute network:

i. **Device count:** Each student will be provided unique login credentials which can be used to connect institute network only on maximum two devices simultaneously. In case, a student wants to connect third device, (s)he will have to log out from the existing device(s) and the connect the new device.

ii. **Antivirus Software:** All computers/devices should have updated antivirus software and should retain the setting that schedules regular updates of virus definitions from the internet.

iii. **OS Updates:** All users must regularly apply operating system updates and patches.

iv. **Administrator Accounts:** All computers available in labs or various locations within the institute should have an administrator account. Administrator accounts should not be used for regular logins.

v. **Password Security:** Follow guidelines for creating strong passwords and change them periodically.

- The password should be difficult to break. Password, defined as:
  a) must be minimum of 6-8 characters in length
  b) must include special characters such as ! $ % & * , . ? + - =
  c) must have at least one capital alphabet and one digit
  d) must not include the characters # @ ‘ “
- Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No., etc.
- Passwords should be changed periodically and also when suspected that it is known to others.
- Do not leave password blank and Mmke it a point to change default passwords given by the software at the time of installation

vi. **Guest Account:** The guest accounts should not have any administrative rights.

vii. **Firewalls:** Enable firewalls on computers. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.

viii. **Software Installation:** Compromised software, if any, must be reinstalled from scratch. Do not install software like Microsoft IIS or turn on any of their functions unless absolutely necessary.

ix. **Backup Strategy:** Implement a regular data backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

x. **Compromised Systems:** Isolate and repair compromised systems as per instructions of the ICT Cell.

xi. **Handling ICT infrastructure:** The users shall not use any device such as podium, mike, projector, biometric; Sound System, CCTV Camera, printers, etc., without permission. Damage to any IT equipment will incur a fine (equivalent to the cost of equipment) on student with warning letter for future.

## 8. Enforcement

Violations of this policy may result in disciplinary action, including termination of enrolment or employment at IIIT Una.

**Disclaimer:**

The ICT Cell shall not be held responsible for loss of any data/information, under any circumstances.

This policy document may be revised without prior notice, and the latest version will be uploaded on the Institute website.