Criterion - 4

Infrastructure and Learning Resources

NAAC- SSR (2nd Cycle)

ETERNAL UNIVERSITY

BARU SAHIB, SIRMOUR-173101
HIMACHAL PRADESH

4.4.2(7)

Policies and Procedures

ETERNAL UNIVERSITY

BARU SAHIB, SIRMOUR-173101
HIMACHAL PRADESH

Classroom Policies

Infrastructure facility

Infrastructure in the class room has been allocated as per the admission of the students in each department. Most of our class rooms are equipped with glass boards and few are smart classrooms. Everyday class rooms cleaned before pursuing the classes.

Timing of the Classes:

Our classes starts onward 9 AM to 5 PM and there is one hour lunch break (1PM to 2 PM) throughout the academic session.

Class attendance

Faculty members are taking attendance regularly on the register as well as on the ERP at each college level. They are conducting classes as per the scheduled time. Time allocated for each class is one hour. Regular class attendance is the basic requirement of the all courses. Students are fulfilling the criteria of 75 per cent of the attendance. Otherwise, they are not allowed to appear in final examination. All instructors are giving warning to all the students in first class regarding the attendance requirement of the course. If students have valid reason to miss their classes, instructors are taking into consideration with consultation of Dean of the respective college. Instructor are giving course outline to students in the first class which includes introduction, objectives of the course, chapter wise distribution of the all course contents, distribution of marks in mid-term, assignment, final exam and the respective time period of each examination.

Cell Phones & Eatables

Cell phones and eatables are not allowed for students in the class rooms.

Dress Code

Dress code is mandatory for only UG students in different colours at each college level.

Course Withdrawal

In case of non-attendance faculty do not withdraw students. It is the responsibility of the students to withdraw the courses officially before the withdrawal deadlines.

Laboratory Policies

Scope: All laboratories in Eternal University.

Policy Statement:

Eternal University is committed to ensuring the safety of its students and employees; and complying with all applicable regulatory environmental, health, and safety requirements. All the departments should to ensure that a minimal level of protection is maintained, all laboratory operations must satisfy all Governmental regulations as well as any guidance developed by Eternal University designated with the authority to do so.

Procedure:

A. General

1. Each faculty member, principal investigator, lab in-charge, lab supervisor or designated responsible authority is responsible for the safety of the individuals working within his or her laboratories.
2. Students should reserve time on the equipment by signing the appropriate schedule.
3. All students must sign and date the log-books for the equipment each time they use it. Faculty in-charge will review the log books on a weekly basis.
4. Food and drinks are strictly forbidden in laboratories.
5. Always keep the laboratory equipment under lock and keep.
6. No laboratory equipment should be removed from the lab without prior permission from faculty in-charge.
7. Appropriate uniform must be worn in laboratories at all times. Long pants and closed-toe footwear are required attire when using any hazardous material or working with animals. Clothing and hair must be secured properly to avoid accidents.
8. An appropriate level of Personal Protective Equipment (PPE) must be worn at all times when hazardous materials such as chemicals, biological materials, radioactive materials, animals or equipment, are used.
9. Proper labeling and storage of all hazardous materials are required and essential for a safe laboratory work environment.

10. Faculty members, principal investigators, lab managers, lab supervisors or designated responsible authorities are responsible for ensuring that all individuals working in their laboratories have been adequately trained.
11. Individuals working in laboratories must have to read and understand all written guidelines, manuals, plans, policies, programs and standard operating procedures that pertain to their activities.
12. Faculty members, principal investigators, lab managers, lab supervisors or designated responsible authorities must follow disposal procedures in compliance with all government regulations and prevent the release of contaminants through sound best management practices for waste generation, handling, and disposal.
13. Safety Data Sheets (SDS) for all laboratory chemicals is required to be maintained in the laboratory.
14. The entrance to each laboratory in which hazardous materials are used or stored shall be posted with the names and phone numbers of the Principal Investigator, Lab Manager, or Lab Supervisor and any other designated personnel who can be contacted in the event of an emergency.
15. The availability and use of a number of types of safety equipment are essential to the practice of safe science. Safety equipment, such as biosafety cabinets, fume hoods, safety showers, fire extinguishers and emergency eyewashes, should be present in well-marked, highly visible, and easily accessible locations in or near all laboratories that use hazardous materials.
16. The prompt reporting of hazardous material spills to proper University authorities is an essential element in the protection of the health and safety of faculty, staff, students, visitors, and patients. Follow the spill procedures for chemical, biological, or radiological spills as necessary.
17. Employees are required to report all occupational injuries, illnesses, or incidents to their work supervisor. Following a report of an incident, the Designated Medical Service Provider for the respective campus shall provide a confidential medical evaluation and follow-up to the employee.

B. Responsibilities

a. University Environmental Health and Safety (UEHS) is responsible for:

1. Developing, implementing, and maintaining all university programs concerning safety and environmental compliance while maintaining appropriate scientific knowledge of the materials, techniques and practices utilized, in collaboration with researchers and experts in the fields UEHS regulates.
2. Assisting faculty members, principal investigators, lab manager, lab supervisor or designated responsible authority with risk assessment and risk mitigation including recommending or requiring safety equipment and PPE as necessary.
3. Performing periodic inspections to confirm compliance.
4. Providing and documenting generally applicable training for laboratory employees concerning the requirements of this policy and their responsibilities;
5. Providing guidance for the preparation of documents and lab-specific training programs required by this policy;
6. Maintaining current knowledge concerning the requirements for storage and use of regulated materials in the laboratory;
7. Investigating injuries, illnesses, or incidents in laboratories and communicating recommendations to appropriate personnel;
8. Participating in research oversight committees and reviewing protocols for safety and compliance;
9. Arranging for individualized medical screenings, surveillance and occupational health services as required;
10. Acting as the point of contact between Indiana University and the governmental entities charged with enforcing the regulatory requirements represented in this policy; and
11. Halting work in laboratories where lack of compliance with requirements represents a danger to individuals

b. Deans, Directors, and Department Heads are responsible for:

1. Ensuring that all departmental faculty and staff members understand and take seriously their roles in implementing the requirements of this policy; and
2. Ensuring an appropriate and safe workspace is provided for work being performed

c. Faculty Members, Principal Investigators, Laboratory Managers, and Laboratory Supervisors are responsible for:

1. Taking overall responsibility for the safety and supervision of individuals working within his or her laboratories;
2. Ensuring that each individual working within the lab is provided with appropriate training on safety and regulatory requirements and ensuring that their laboratory personnel receive the appropriate procedure-specific instruction and are proficient at performing those procedures;
3. Ensuring that each individual working within the lab is provided with any needed medical surveillance and/or medical support services required by their work;
4. Ensuring that required safety equipment and personal protective equipment are provided, maintained, and used;
5. Ensuring that specific standard operating procedures incorporating safety considerations are developed and observed;
6. Ensuring that prompt action is taken to correct any unsafe acts or conditions which have been observed or reported, whether through inspections or other routes;
7. Notifying IUEHS in the event of an injury or illness that occurs in the laboratory; and
8. Being familiar with reading, understanding, and implementing all requirements associated with specific programs.

d. Individuals within Laboratories are responsible for:

1. Complying with all safety requirements for the work being performed;
2. Participating in required training and medical programs
3. Wearing appropriate lab apparel and using personal protection equipment (such as lab coat, safety glasses, gloves, etc.);
4. Utilizing the appropriate safety equipment properly (such as the fume hood);
5. Reading, understanding, and following the established standard operating procedures;
6. Obtaining information prior to using an unfamiliar hazardous material or performing a new task; and
7. Informing the faculty member, principal investigator, lab manager, lab supervisor or designated responsible authority of any accident or unsafe conditions.

COMPUTER LAB RULES

Come in to the lab quietly and go to your assigned computer. Do not touch other keyboards or mice on the way to your computer. Read board and begin assignment if one exists or wait for instructions before you do anything.

Only visit approved internet sites and only when you have permission to do so. Do not download anything unless told to do so. Never give out personal information. Do not share your passwords with anyone other than your parents or teachers, if college related. If you see anything that makes you feel uncomfortable turn off monitor and let your teacher know immediately. Do not show to your friends first.

Make sure you leave your workspace as you found it. Exit out of all programs. Hang up your headphones. Straighten your keyboard and mouse. Push in your chair/stool. Collect and throw away any trash on your way out. Take your belongings and anything you have printed with you when you leave.

Print only if you have permission. Only press the print option once.

Use only your assigned computer. Do not move the icons on the desktop. Do not change any system settings without permission. Do not edit files that do not belong to you. Help others with your mouth and not their mouse.

Treat your classmates your teacher and all equipment with respect. Help your neighbor if they need help. Do not talk when your teacher is talking. Come to the computer lab with clean hands. If you have just had recess or lunch please wash and dry your hands before you come to the lab. No banging your mouse, or banging the keys on your keyboard,

Eat and drink outside of the lab only. No food or drink allowed in the lab.

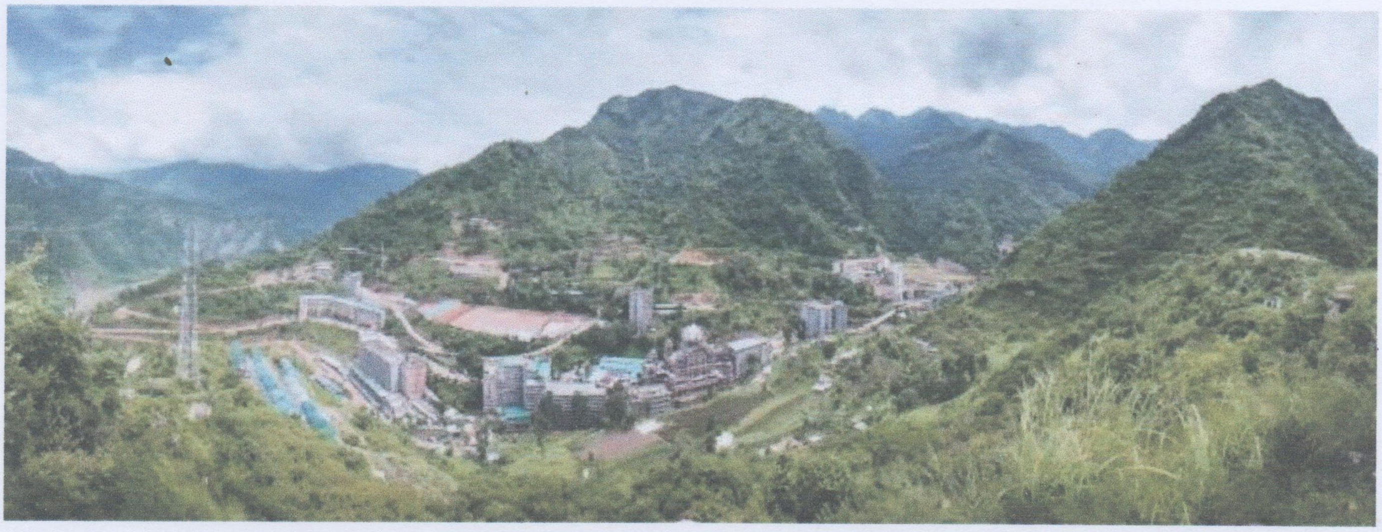
Read the screen before asking questions.

ETERNAL UNIVERSITY STUDENTS' GUIDE

THIRD ORDINANCE

Contents

IT POLICY



Eternal University, Baru Sahib

INFORMATION TECHNOLOGY INFRASTRUCTURE USAGE POLICY

Introduction

Students, Teaching and Non - Teaching Staff, Management and visiting Guests and Research Fellowship Members of Eternal University 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.

General Rules

1. Students, Teaching and Non - Teaching Staff, Management and visiting Guests and Research Fellowship Members are authorized to use the computing, networking, and other IT facilities for academic purposes, official university business, and for personal purposes as long as such use does not violate any law or any university policy.

2. The University prohibits its users from gaining or enabling unauthorized access to forbidden IT resource on the University network. Any such attempt will not only be the violation of University Policy but may also violate national and international cyber laws, provisions under The Information Technology Act of India and infringe the principals of National Cyber Security Policy, and subject the user to both civil and criminal liability. However, the University reserves all the rights to access and analyze the IT resource and Information for any legal and/ or institutionally provisioned operation, on its own or through its affiliates.

3. The University prohibits its users from sending, viewing or downloading fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or University policy. Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful e.g. when such content is received through e-Mail etc. As a generalized policy, any contribution towards the destruction or distortion of congenial academic or work environment is prohibited.

4. Users must not violate various IPR and copyright law(s), and licensing policies as associated with copyrighted materials and software. Any unlawful file- sharing, use of any form of illegal or pirated or un-licensed software, on the University's IT resources (including individually owned IT resource being used under Institutional IT privileges) is strictly prohibited and any such act shall constitute a violation of the University policy.

5. University also recommends its students, faculty and office staff, to use Open-Source Operating Systems (OS) and Processing Software (PS) such as Ubuntu/ CentOS or other and Libra Office/ OpenOffice/ WPS Office, respectively. Further, users of the computers sponsored directly or indirectly by Eternal University should migrate on the recommended OS & PS as their primary software and should generate expertise on it. In case of technical limitation in such adaptation, relaxation may be requested from competent authority on valid grounds.

6. By agreeing to abide by the terms of use of various online media forums, the users are expected to adhere with the norms as prescribed by respective social networking websites, mailing lists, chat rooms, blogs, unless a user has proper authorization, no user should attempt to gain access to information and disclose the same to self or other unauthorized users. The broader concept of data privacy must be honored by each user.

7. No user should attempt to vandalize, damage or change any data inappropriately, whether by accident or deliberately. The basic notion of trustworthiness of information resources must be preserved by all of its users. Any interference, disruption or encroachment in the University IT resources shall be a clear violation of the University policy.

8. No user should attempt to affect the availability of IT resource, whether accidently or deliberately.

9. As long as individual departments, Hostel, individual units etc. can retain consistency in compliance of the IT (Usage) Policy, Eternal University, they may further define and implement additional "conditions of use" for IT resources under their control. It will be the responsibility of the 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 (Usage) Policy of the University.

10. As a part of certain investigation procedures, the University may be required to provide its IT information, resource and/ or records, in parts or full, to third parties. Also, for proper monitoring and optimal utilization of University IT resources, the University may review, analyze and audit its information records, without any prior notice to its Users. Further, the University may also seek services from third-party service providers. Accordingly, the users can only have reasonable expectation of privacy on the University's IT resources.

11. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems.

12. No food or drink is permitted in the laboratories. Also making noise either through games/music/movies or talking and/ or singing loudly (the list is not exhaustive) is prohibited.

13. Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate. Depending upon the nature of the violation, the University authorities may take an action.

14. The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through the news groups.

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging with their User **ID** and **password**. For obtaining the university's email account, user may contact IT Department for email account and default password by submitting an application in a prescribed proforma.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. 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 software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. 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.
4. Users should configure messaging software 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.
5. 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.
6. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
7. 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.
8. Impersonating email account of others will be taken as a serious offence under the university IT security policy.

9. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

10. Once the faculty has departed from the university service, the administrator must delete or terminate the email accounts to prevent abuse.

Social Media Policy

POLICY

- This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include What's App, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others.

PROCEDURES

- The following principles apply to professional use of social media on behalf of Eternal University as well as personal use of social media when referencing Eternal University.
- Employees need to know and adhere when using social media in reference to Eternal University.
- Employees should be aware of the effect their actions may have on their images, as well as Eternal University's Image. The information that employees post or publish may be public information for a long time.
- Employees should be aware that The University may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to Eternal University, its employees, or customers.
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment or which may hurt religious & Sentiments of any one or any Community.
- Employees are not to publish post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the VC Office.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to the authorized University spokespersons.
- If employees encounter a situation while using social media that threaten to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of VC Office.
- Employees should get appropriate permission before they refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Social media use shouldn't interfere with employee's responsibilities at Eternal University. The University's computer systems are to be used for business purposes only. When using University's computer systems, use of social media for business purposes is allowed only to those staff whose work profile requires use of social media (ex: Face book, Twitter, Eternal University blogs and LinkedIn, What's app, Instagram, any other) , but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.

- Subject to applicable law, after---hours online activity that violates or any other company policy may subject an employee to disciplinary action or termination.
- It is highly recommended that employees keep Eternal University related social media accounts separate from personal accounts, if Possible.
- Employees should not use any type of offensive /abusive language or make any comment/post any photo which is not in line with their image as a faculty/Teacher (As they belong to a very respected community).

Responsibilities of University IT Department

A. **Maintenance of Computer Hardware & Peripherals**

IT DEPARTMENT is responsible for maintenance of the university owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Department.

B. **Receiving Complaints**

IT DEPARTMENT may receive complaints from User, if any of the particular computer systems are causing network related problems.

IT DEPARTMENT may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in IT DEPARTMENT receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

C. **Scope of Service**

IT DEPARTMENT will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the university and was loaded by the company.

D. **Installation of Un-authorised Software**

IT DEPARTMENT or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

E. **Reporting IT Policy Violation Incidents**

If IT DEPARTMENT or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the university, such incidents should be brought to the notice of the university authorities.

F. **Reporting incidents related to Network Operations**

When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the IT DEPARTMENT.

G. **Rebuilding the Computer System**

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.

Guidelines for Desktop Users

These guidelines are meant for all members of the EU Network User Community and users of the University network.

Due to the increase in hacker activity on campus, University IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

1. All desktop computers should have the latest version of antivirus such as Microsoft Windows Defender or any other 3rd party Anti-virus and should retain the setting that schedules regular updates of virus definitions from the central server.
2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, security policies should be set at the server level and applied to the desktop machines.
3. All Windows desktops (and OS X or Open-Source OS) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.
4. The password should be difficult to break. Password, defined as:

i. must be minimum of 6-8 characters in length.
ii. must include punctuation such as ! $ % & * , . ? + - =
iii. must start and end with letters.
iv. must not include the characters # @ ' " `
v. must be new, not used before
vi. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No.etc.

5. passwords should be changed periodically and also when suspected that it is known to others.

i. Never use 'NOPASS' as your password ii.Do not leave password blank and Make it a habit to change default passwords given by the software at the time of installation

6. The password for the user login should follow the same parameters outlined above.
7. The guest account should be disabled.
8. New machines with Ubuntu or Windows should activate the built-in firewall.
9. 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.
10. In addition to the above suggestions, IT Department recommends a regular 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.
11. If a machine is compromised, IT Department will shut the port off. This will isolate the computer, until it is repaired as per the guidelines. At that time, the port will be turned back on.

Video Surveillance Policy

The system

1.1 The system comprises: Fixed position cameras; and Zoom cameras; Monitors: Multiplexers; digital recorders; HDD Storage; Public information signs.

1.2 Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

1.3 Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.

1.4 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.

2.0 Purpose of the system

2.1 The system has been installed by university with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order.
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is or is threatened to be taken.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment

The system will not be used:

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

2.2 Covert recording

2.2.1 Covert cameras may be used under the following circumstances on the written authorization or request of the Senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorized or illegal activity is taking place or is about to take place.

2.2.2 Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorized activity.

2.2.3 The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

3. Complaints

3.1 It is recognized that members of university 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 Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralized Complaints Procedure by

3.2 obtaining and completing a University Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer, these rights do not alter the existing rights of members of university or others under any relevant grievance or disciplinary procedures.

9-04-2024

Appendix – I: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID

(For Teachers & Staff only)

First Name	:
Middle Name	:
Last Name	:
Department/ Branch	:
Current Email address*	:
Mobile Number	:

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department/ Controlling Officer.
4. An official Email address would be created within 48 hrs. - 72 hrs.
5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department/ Controlling Officer)

Appendix – II: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID

(For Research Scholars only)

First Name	:
Middle Name	:
Last Name	:
Department	:
Name of the PI	:
Name of the Project	:
Duration of Research	:
Current Email address*	:
Phone Number	:
Enrollment Number	:

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department and Principal Investigator.
4. An official Email address would be created within 48 hrs. - 72 hrs.
5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department)

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Principal Investigator)

Appendix – III: Wi-Fi Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS

(For Students only)

Name	:	
Father's Name	:	
Gender	:	
DoB	:	
Department	:	
Course	:	
Semester	:	
Enrollment No.	:	
Emailaddress*	:	
MobileNumber	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department.

(Signature of the Head of the Department)

University Library Rules

i. Maximum of two books will be issued to undergraduate students for a period of 10 (Ten) days.

ii. Maximum of three Books will be issued to postgraduate students for a period of 14 (fourteen) days.

iii. An overdue charge @Rs.5/- per day will be levied after the expiry of due date.

iv. Reserve textbooks are issued only for an overnight from 7.00 pm to 9.00 pm and are to be returned in the morning before 9.00 am. Overdue fine for such books is Rs 50/- per hour.

v. The overdue charges can only be reduced or remitted by the Vice Chancellor or his nominee.

vi. Books having same title will not be issued simultaneously.

vii. A book once returned by a student will not be issued to the same student on the same day.

viii. Reference Books, Previous Years Question Papers, Syllabus, Magazines/ Journals will be issued for Photostat purpose only for 30 minutes.

ix. Students must carry their Identity Card with them at all times in the Library. On their cards if a member of staff requests them to do so, it is mandatory to show at the time of Issue – return of books.

x. Any book damaged, marked, misplacing of pages etc. should be brought in the notice of Librarian at the time of issuing otherwise person who gets it issued will be responsible.

xi. Books can be recalled at any time in case of an urgent demand for the same, by the other users.

xii. The Librarian may amend the library rules and regulations as and when necessary with the consultation of Library Committee.

Lost / Damaged Library Documents

i. Student will be fully responsible for loss or misuse of book. If the book is lost, an immediate report should be made to the Librarian to enable appropriate action to be taken.

ii. In case of lost or damage of the book, borrower has to pay double the cost of book along with overdue and other charges applicable as per rules.

iii. Entire volume cost will be recovered for the document which is a part of multi volume/issue/set.

Library Timings

i. The library will remain open on all days of the year except on national holidays i.e. Jan 26th, Himachal Day April 15th, August 15th and Oct 2nd. On working days, it will open from 8.30 am to 9.00 pm and on Sunday from 8.30 am to 5.30 pm.

ii. Books Issuing/Return Timings: Monday to Saturday (9.00 am to 12.30 noon) and (4.00 pm to 6.00 pm); on Sunday (9.00 am to 12.30 noon)

Scientific Journals (Use Online):

Eternal University Library has renewed the J-Gate portal of e-Journals from 25.08.2020 to 24.08.2021. This portal of e-journals includes huge range of articles on the following subjects

*Agricultural & Biological Sciences

*Basic Sciences

*Biomedical Sciences

*Engineering & Technology

* Social Sciences

Sports Policy

Eternal University has constituted a sports committee. The aims and objectives of the sports committee are as:

1. To organize and regulate sports activities within the jurisdiction of the University, and inter University tournaments.
2. To promote the best type of sportsmanship and team spirit among the alumni of the University.
3. To conduct Annual Tournaments in various sports events for students to all the colleges of the university in accordance with the rules made by the sports committee and ratified by Academic Council.
4. To Promote drug free sports.

Rules for Participants:

1. Participants will carry their own sports kit as per their sports activity.
2. A participant can compete for maximum 3 activities during athletic meet.
3. Wearing of proper kit is compulsory for all the participants to compete.
4. All the interested participants will register themselves with respective sports coordinator at least four days before the event.
5. Presence of all the participants is mandatory; in case of absence, their candidature will be cancelled.
6. The decision of 3-member committee for Jury in case of any misunderstanding is final.