INFORMATION TECHNOLOGY POLICY

Bundelkhand University
Kanpur Road, Jhansi- 284128, Uttar Pradesh, India

FROM THE DESK of VICE CHANCELLOR

Welcome to Bundelkhand University, Jhansi

In digital era, the Bundelkhand University has develop its IT resources to facilitates its stakeholders. To make it sustainable, the advancement in IT resources as well expandable systems are being installed within the campus. The University has adopted the Information Technology Policy so far. I am happy to share print version of the IT policy for its users. I am sure that this policy will keep strict vigil on the university IT resources. I extend good wishes to all.

Prof. Mukesh Pandey
Vice Chancellor
Bundelkhand University Jhansi (UP), India

Established on 26th August, 1975, bundelkhand University is emerging as a prominent centre of higher learning encompassing more than 120 courses in 9 Faculties with 27 institutes and 38 departments. It is delivering education to more than 9 thousand students on campus and 3 lac students in its 367 affiliating colleges.

Recognized as **Number One University** by the State Government of Uttar Pradesh consecutively for three academic years, it is the only premier institution which has been **accredited three times by the NAAC** with B++, listed in **68th rank in NIRF** for Pharmacy and is **certified with ISO 9001** for Quality Management Services.

VISION

The University aims to become a world-class institution by tapping human potential to lead the country in changing national, regional and global scenario.

MISSION

To impart quality vocational and scientific education through basic and applied research, to improve the quality and value of human irrespective of gender, caste, nationality and religion.

Information Technology Policy

Bundelkhand University
Kanpur Road, Jhansi-284128 (U.P.) INDIA

Bundelkhand University
Kanpur Road, Jhansi-284128 (U.P.) INDIA

Information Technology Policy

Introduction

Students, Teaching and Non – Teaching Staff, Management and visiting Guests and Research Fellowship Members of Bundelkhand 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. If any of the members mentioned above use any of the University IT Resources, acceptance to this IT Policy is by default assumed an its strict following is mandatory for every user.

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 wil 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 principales 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 resrouce 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, obscence (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 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/Cent OS or other and Libra Office/Open Office / WPS Office, respectively. Further, users of the computers sponsored directly or indirectly or indirectly by Bundelkhand 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 reqested 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, bloogs, Unless, a user has proper authorization, no user should attempt to gain access to information and disclosed the same to self or other unauthorized user The broader concept of data privacy must be honoured by each user.

7. No user should attempt to vandalize damage or change any dada inappropriately, whether by accident or deliberately. The basic notion of trustworthiness of information resoures 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, invididual units etc. can retain consistency in compliance of the IT (Usage) Policy, Bundelhand 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 requird 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. User 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. Tempering to any IT Resources will be treated as violation of this IT Policy and appropriate action against violator may be taken.

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 probibited.

13. Violations of policy will be treated as academic misconduct, misdemeanour, 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.

15. Any criminal activity through Computer/IT Resources will be cover under IT Act 2005.

16. University uses DNS/DHCP/Proxy for providing networking resources to Stake Holders.

17. VPN/Web-Proxy or any other mode of network by pass is strictly prohibited in the Campus Network which will be treated as violation of policy.

18. Any Ethical Hacking activities or Uses Network Traffic Analyzing softwares is strictly probibited which will be treated as violation of policy.

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 administrations, 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 commnunications 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 should apply for an online application under their University login by selecting Email Services under Computer Center Eservices Module.

Users may be aware that by using the e-mail 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 purpose 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 of fraudulent messages / images.
3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. 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 messges may contain viruses that have potential to damage the valuable information on your computer.
6. 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.
7. 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.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

9. 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 peeing into its contents, by the user who has occupied that computer for its use.

10. Impersonating email account of others will be taken as a serious offence under the university IT security policy.

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

12. Faculty / Staff/Students while leaving the University should ensure to get their E-mail ID's deactivated from computer center. Using official E-mail ID after leaving University is not permitted and would be treated as violation of policy.

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 formums, 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 Bundelkhand University as well as personal use of social media when referencing Bundelkhand University. Employees nee to know and adhere when using social media in reference to Bundelkhand University.

- Employees should be aware of the effect their actions may have on their images, as well as Bundelkhand University's Image. The information that employees post or publish may be public information for a long time.

- Employees should be aware that the Univeristy 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 Bundelkhand University, its employees, or stakeholders.

- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietory, harassing, libellous, or that can create a hostile work envoironment or which may hurt religious & Snetiments 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 Human Resources Department.
- 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 Human Resources Department.
- 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 Bundelkhand University. The University's computer systems are to be used for business purposes only. When using University's computer system, use of social media for business purposes is allowed only to those staff whose work profile requires use of social media (ex: Facebook, Twitter, Bundelkhand University blogs and Linkedin, WhatsApp, 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 University policy may subject an employee to disciplinary action or termination.
- It is highly recommended that employees keep Bundelkhand 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 beloging to a very respected community).

Responsibilities of University Computer Center

A. Maintenance of Computer Hardware & Peripherals

Computer Center is responsible for maintenance of the university owned computer systems and peripherals that are neither under warranty nor annual maintenance contract, and whose responsibility has officially been entrusted to Computer Center.

B. Receiving Complainants

Computer Center may receive complaints from the users if any of the University owned computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in Computer Center may receive complaints from the users of Univeristy owned computer systems under warranty / AMC 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

Computer Center 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 OEM or University.

D. Installation of Un-authorised Software

Computer Center 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 Computer Center 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 Computer Center and university authorities.

F. Reporting incidents related to Network Operations

When the network port of any particular computer system is turned off due to unauthorized user network device, virus or related activity that is affecting the network performance, the same will be informed to the COMPUTER CENTER. After taking necessary corrective action

service engineers should inform Computer Center about the same, so that the port can be turned on by Computer Center.

G. Rebuilding the Computer System

When the service engineers reformat the computer system 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. All users should take periodic backup of important data. Computer Center will not be responsible for any data loss due to system failure Computer Center may facilitate the user in data backup task if support is asked for the same but taking data backup will be responsibility of respective user. Computer Center will not be responsible for backup or restoration of data.

H. Coordination with INTERNET UNIT

Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the networks or the software installed or hardware malfunctioning, service engineer may coordinate with Computer Center staff to resolve the problem with joint effort. This task should not be left to the individual user.

Guideline for Desktop/Laptop Users

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

Due to the increase in hacker activities 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 Symantec Anti-Virus (PC) or Quick Heal 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 additional, 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 desktop (and OS x or later Macintosh desktop) should have an 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 incude special characters 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., or DOB 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 point 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. Built-in-firewall should be enabled.

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. All the software on the compromised computer systems should be re-installed from scratch.

11. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.

12. In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.

13. In addition to the above suggestions, Computer Center 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.

14. If a machine is compromised, Computer Center 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.

15. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, Computer Center technical personel can scan the servers for vulnerabilities upon request.

Video Surveillance Policy

1.0 **The system**

1.1 The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS 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 proctors 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 reuest of the higher authorities.

- 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 unauthorised 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.

3.0 The Security Control Room

3.1 Images captured by the system will be monitored and recorded in the Security Control Room, “the control room”, twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

3.2 No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the respective employee, authorized members of senior management, police officers and any other person with statutory powers of entry.

3.3 Staff, students and visitors may be granted access to the Control Room on a case by-case basis and only then on written authorization from the higher authorities. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room.

3.4 Before allowing access to the Control Room, staff will satisfy themselves of he identity of any visitor an that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitor log, which shall include details of their name, their department or organization they represent the person who granted authorization and the times of entry to an exit from the centre. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

4.0 Security Control Room Administration and Procedures

4.1 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.

4.2 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.

5.0 Staff

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.

6.0 Recording

6.1 Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

6.2. Image will normally be retained for ten days from the date of recording and then automatically over written and the Log updaed accordingly. Once a hard drive has reached the end of its use its will be erased prior to disposal and the Log will be updaed accordingly.

6.3. All hard drives and recorders shall remain the property of university until disposal and destruction.

7.0 Access to images

7.1. All access to images will be recorded to the Access Log as specified in the Procedures Manual.

7.2 Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

7.3.0 Access to images by third parties

7.3.1 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;

- Law enformcement agencies where images recorded would assist in a criminals enquiry and/or the prevention of terrorism and disorder.
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of he general public is required in the identification of a victim of crime or the identification of a perpetrator of crime.
- People whose image have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency service in connection with the investigation of an accident.

7.4.0 Access to images by a subject

CCTV/IP Camera digital images, if they show a recognizable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by

C.C.T.V. /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.

7.4.1 A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the higher authorities. Subject Access Request can be made in office hours from Monday to Saturday, except university is officially closed.

7.4.2 The Computer Center will then arrange for a copy If the data to be made 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. All communication must go through the university Computer Center. A response will be provide promptly and in any event within forty days of receiving the application.

7.4.3 The Data Protection Act gives the Computer Center 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.

7.4.4 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.

8.0 Request to prevent processing

8.1 An individual has he right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

8.2 All such requests should be addressed in the first instance to the higher authorities, 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.

9.0 Complaints

9.1 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 higher authorities. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralised Complaints Procedure by obtaining and completing a University Complaints Form and copy of the procedure. Complaints forms may be obtained from the Registrar’s Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Computer Center; these rights do not

alter the existing rights of members of University or others under any relevant grievance or disciplinary procedures.

ICT Resoure Demand/Maintenance/Procurement Policy

1. Demand

- All user demands will be forwarded to Computer Center. After analyzing User & Requirement of User Computer Center will suggest specification for IT resource to be provided.
- There will be category for Desktops/Laptop namely High End, Mid-Range and Entry Level based on uses and User Category.
  - IT/Technology Department will be allowed High End Resource for all faculties and Mid-Range Resource for Non-Teaching Staff.
  - Other Departments will be allowed Mid-End Resource for Associate Professor or above Level and Entry Level Resource for Assistant Professor Level and Non-Teaching Staff.
  - Printer and Scanners will be allowed to Deans/HOD's/Coordinators and Department and standalone Offices only.
  - Administrative Officers Such Vice Chancellor/Finance Officer/Registrar/ Examination Controller/Deputy Registrar will be allowed high End Resources with Printer & Scanner. Assistant Registrar will be allowed mid-range resources with Printer and Scanner.
  - Standalone offline/online UPS will be allowed only if Centralized un-interrupted power supply is not available.
  - Servers/Work Station and High End Resources may be allowed in-case of Project grants and if Requirement of such resource is justified and permitted by the Higher Authority.

2. Maintenance

- IT Resources not under warranty or AMC by third party will be maintained by IT Support Engineer of Computer Center.
- In-Case of Hardware Failure any procurement would be done as per recommendation of Computer Center.

- Any IT Resource under warranty or outside warranty will not be opened/termpered/ mishandled by user of that resource.

3. Procurement

- As per above point-1 Demand, the resource available in the Central Store/Departmental Store would be assigned to respective user after approval of Competent Authority.
- If resource not available than procurement of the resource as per the recommendation of computer center will be done as per the University/Govt. procurement rules and regulations.

DECLARATION

I, _____ Employee ID/Enrollment No. _____ do hereby declare that as a Employee/student in Bundelkhand University will abide by the above mentioned rules. I accept that any act of mine that can be considered to be the violation of the policy will be dealt with as mentioned in rule #13.

Date: _____ Signature:

Smt Anandiben Patel
Hon'ble Chancellor & Governor of Uttar Pradesh

Yogi Aditya Nath Ji
Hon'ble Chief Minister UP Govt.

Estd. 1975

Shri Yogendra Upadhyay
Higher Education Minister of Uttar Pradesh

Smt. Rajni Tiwari
State Higher Education Minister of Uttar Pradesh

Prof. Mukesh Pandey
Vice-Chancellor

BUNDELKHAND UNIVERSITY, JHANSI (U.P.)

● B++ NAAC Accredited, NIRF Ranked, ISO Certified ● Ranked as Number 1 University in U.P.

N.E.P.-2020 Applied on courses as per Uttar Pradesh Government orders

Science Faculty

B.Sc. Courses for Campus Only:- Maths Group (PCM) – (DA), Biology Group (ZCB) – (DA)

(Hons.) Courses : Biochemistry** – (DA), Biotechnology** – (DA), Microbiology** – (DA), Forensic Science – (DA), Geology – (DA), Biomedical Science– (DA), Food Technology** – (DA), Maths Statistics & Computer Science. – (DA), Environmental Science - (DA), B.C.A. (Bachelor of Computer Applications) – (DA)

P.G.D.F.S. (Post Graduate Diploma in Forensic Sc. – (DA) , Home Science (DA)

Advance Diploma in Data Science - (DA)

Advance P.G. Diploma in Microbiology and Food Technology - (DA)

P.G.D.E.M.: (Post Graduate Diploma in Environmental Management)– (DA)

M.Sc Courses:- Mathematics** - (ET), Statistics - (DA), Food Technology** - (ET), Biochemistry - (DA), Biotechnology - (DA), Microbiology- (DA), Biomedical Science- (DA), Physics** - (ET), Electronics - (DA), Chemistry** - (ET), Botany** - (ET), Zoology** - (ET), Forensic Science, - (ET), Environmental Science - (DA), Ayurveda & Alternate Medicine- (DA), Geology – (DA), Home Science (Food & Nutrition) – (DA), Home Science (H D.F.S.) – (DA), Life Science - (DA)

Agricultural Faculty

B.Sc. (AG.) Hons. Course : B.Sc. Agriculture Science**– (ET)

M.Sc. (Ag) Courses: Agro Forestry – (ET), Horticulture – (ET), Plant Pathology** – (ET), Entomology** – (ET), Genetics & Plant Breeding**– (ET), Agricultural Extension – (ET), Seed Technology – (ET), Agronomy** – (ET), Soil Science & Agricultural Chemistry** – (ET), Animal Husbandary & Dairying* – (ET), Agricultural Economics**– (ET)

Medical Faculty

D. Pharm. - (ET),

M. Pharm. (Pharmaceutics) - (ET), **M. Pharm.** (Pharmacognosy) – (ET),

B.P.T. (Bachelor of Physiotherapy) – (ET)

B.Sc. - M.L.T.## (Bachelor of Science in Medical Laboratory Technology)- (DA) (Approved by the UP Government and UP State Medical Faculty)##

Architecture Faculty

B- Des (Interior Design) - (DA)

Art Faculty

B.A.: Courses for Campus Only

B.A.: Mass Communication and Journalism** – (DA)

B.F.A. : Drawing & Painting –(DA) Commercial Arts) – (DA)

B.A. (Hons.) Courses: Hindi – (DA), Social Work – (DA), English – (DA), Education – (DA),Economics – (DA)

B.Lib. & I.Sc. **– (DA)

B.P.E.S.: (Bachelor in Physical Education & Sports) – (DA)

B.P.Ed. – (ET)

M.P.E.S. (Master in Physical Education & Sports)- (DA)

P.G.D.E.M.: (Post Graduate Diploma in Electronic Media) – (DA)

M.A. Courses: Hindi – (DA), Home Science – (DA), Education – (DA), English – (DA), Drawing & Painting, – (DA), Mass Communication & Journalism – (DA),

M.Lib & Information Science – (DA)**

M.F.A. (Master of Fine Arts in painting). –(DA)

M.F.A. (Master in Fine arts in applied art) - (DA)

M.A. Applied Economics (Master of Arts in Applied Economics) – (DA)

MBA Business Economics (Master of Business Administration in Business Economics) – (ET)

M.S.W. (Master of Social Work) – (DA)

Commerce Faculty

MBA Banking & Insurance (Master of Business Administration in Banking & Insurance)– (ET), **B.B.A.(HONS.)** – (ET), **B.Com. (HONS.)** – (ET), **B.B.A.** (Tourism) – (DA), **M.Com** (Finance) – (DA)

Education Faculty

M.Ed.,-(ET),**
B.Ed.#** (Bachelor of Education)
B.El.Ed.* (Bachelor of Elementary Education)-(ET)
ET - Entrance Test
DA - Direct Admission through Merit

Law Faculty

B.A.L.L.B** (Integrated) – (ET)
LL.B** , – (ET)
L.L.M.** – (ET)
*** Only in Affiliated Colleges**
**** Also in Affiliated Colleges**
 # Through state level Entrance Examination Only

Ph.D. Programme in 44 Subjects

Wasi Mohammad
Finance Officer

Vinay Kumar Singh
Registrar

Raj Bahadur
Controller of Examinations

Technical & Management Courses

Architecture: B.Arch. (Bachelor of Architecture),
Pharmacy: B.Pharm.
Engineering: B.Tech. (Computer Science, Electronics & Comm., Bio-Tech)

Admission on 100% seats through A.K.T.U. Counselling (JEE MAINS, C.U.E.T., N.A.T.A. TEST)

M.B.A. - (ET), **M.B.A.** (International Business) - ET), **M.B.A.** (Tourism) - (ET), **M.B.A.** (Financial Management) - (ET), **M.C.A.** - (ET), **B.Tech.** (Food Engg. Technology) - (ET), **B.Tech.** (Electronics & Instrumentation)-(ET), **B.Tech.** (Bio-Medical)- (ET), **B.Tech.** (Mechanical Engg.) - (ET), **Integrated - B.H.M.C.T. - M.H.M.C.T. -** (Bachelor/Master in Hotel Management & Catering Tech.) - (ET)

Admission on 50% seats through BU Entrance Test and on 50% seats through A.K.T.U. Counselling

Territorial Jurisdiction of Bundelkhand University

Type of College	Total	Accredited
Government Colleges	23	6 (4 in process)
Aided Colleges	13	7 (2 in process)
Self Finance Colleges	331	21 (10 in process)

Bundelkhand University
Kanpur Road, Jhansi–284128, Uttar Pradesh, India
Tel.: 0510–2320497, 2321158 | Fax : 0510–2320761
registrar.bujhansi@gmail.com I www.bujhansi.ac.in
@BUJHSOFFICIAL @busocial

Compiled by : Prof. Avanish Kumar
Prepared by : Dr. Deepak Tomar, Dr.Zakir Ali, Dr. Sadik Khan