



# Dr. B. R. AMBEDKAR OPEN UNIVERSITY

Prof. G. Ramreddy Marg, Jubilee Hills, Hyderabad - 500 033  
Centre for Internal Quality Assurance (CIQA)

**Information  
Technology  
Policy**



# B R A O U

## ABOUT THE UNIVERSITY

The University, initially known as Andhra Pradesh Open University, was set up on 26th August 1982 through an Act of the A.P. State Legislature (APOU Act 1982). Subsequently, the University was renamed as Dr. B.R.Ambedkar Open University on 26 October, 1991 by the Government of Andhra Pradesh. The establishment of this University, the first of its kind in India, heralded an era of affirmative action on the part of the Government of Andhra Pradesh to provide opportunities of higher education to all sections of society to meet the changing individual and social needs. The University offers services to defense personnel, prison inmates and learners from remote and tribal areas who are not having access to education. All the programmes offered by the University are recognised by the University Grants Commission, New Delhi. The motto of the University is "EDUCATION FOR ALL". The university is adapting all the latest ICTs regarding teaching, learning and evaluation to reach the unreached.



- ◆ Enrichment of ongoing academic programs.
- ◆ Competency building through education and training programs. Interactive individual-based teaching-learning processes.
- ◆ Reliable and credible student evaluation systems.
- ◆ Result-oriented, accountable, and transparent administrative and logistic support systems. and
- ◆ Research, innovation, training, and networking for system development and staff development.



Dr. B. R. Ambedkar's social philosophy of education as a means of creating an egalitarian society is the vision of this University. Access to relevant, quality education and training programs for diverse sections of society with a focus on hitherto deprived sections at lower costs by using modern technologies in teaching-learning processes as well as in administrative and support services is the goal of this University. The University programs aim at making education and training instruments for living and for making a living.

# Information Technology Policy

## INTRODUCTION

Dr. B.R. Ambedkar Open University (BRAOU), formerly known as Andhra Pradesh Open University, is located in the city of Hyderabad. With a wide network of study centers spread throughout the states of Telangana and Andhra Pradesh, the University has its motto "Education at Your Doorstep". The University, the first of its kind in the country was brought into being through an act of the Andhra Pradesh State Legislature in August, 1982. At present, the University is offering learner support services through 180 Learner Support Centers (LSCs) spread across the two Telugu states.

Dr. B.R. Ambedkar's social philosophy of education as a means of creating an egalitarian society is the vision of this University. Giving access to quality education and training programs for diverse sections of society with a focus on deprived sections at lower cost by using modern technologies in teaching-learning processes as well as in administrative and support services is the goal of this University. The University programs aim at making education and training instruments for living and for making a living.

To support the University's vision and mission, the University established a Computer Centre in 1994 to provide IT support services to the University. The University has framed an IT policy to enable the University to provide IT-enabled services to the learners and staff.

## PURPOSE

The University recognizes the vital role that Information Technology plays in the University's administrative activities as well as the importance of protecting information in an academic environment in all forms. As more information is used and shared in a digital format by students, Faculty, and staff, both within and outside the University, increased efforts must be made to protect the information and the technology resources that support it. Increased protection of our Computer and Communication resources to ensure the usability and availability of those resources is the primary purpose of this policy. The ethical principles that apply to everyday community life also apply to computing and communications. Every user of the university has two basic rights: privacy and a fair share of the available resources. It is unethical for any person to violate these rights.

The Policy lays down general guidelines for the use of computing and communication resources.

### 1. Policy Applies to

This policy applies to all the staff members of the University including

- All the University employees, who are accessing the University network with an electronic device provided by the University or through their private devices.
- All the students, who are accessing the University website with their credentials.
- All the students, who are practicing /attending exams in the University LABs.
- All the vendors who are supplying IT-related equipment, providing AMC, and supplying software.
- All those who access University Information Technology Resources, whether affiliated with the University or not, whether on campus or from remote locations, including but not limited to students, Faculty, staff, contractors, consultants, temporary employees, guests, and volunteers.

## 2. IT-enabled Services

The University provides online services to the learners including online admissions, online examinations registration, online payments (Debit/Credit cards/ APT Online franchise system), downloading Hall tickets, marks memos, statements of activities, course material, online requests for data correction, online registration for Certificates, etc. The University allows the learner to download their details using OTP authentication.



Learners and the University communicate with each other through different channels through SMS, email, and by logging on to the University website using their credentials and OTP. The University is always trying to improve its communication system with its learners.

Online services are also extended to the Learner Support Centre to download required data from the University portal on-demand including Nominal rolls for exams, and admissions details. LSCs are extending learner support services using social media (WhatsApp, Telegram App) and SMS-based services. The IT policy also covers the delivery of IT-enabled services to learners and other stakeholders.

**The following are the IT-enabled services:**

Providing admission and examination registrations through online mode to reduce the paperwork of the learners and staff.

Online Fee Collection System (collecting various types of fees through Debit/Credit cards, internet banking, UPI payments, etc.)

IT Support for the blended mode of counseling; one for offline classes at Learner Support Centers and the other for Online mode of teaching. Recorded Audio/Video lessons are posted on the University website for learners' ready reference.

Hosting Audio/Video lessons on the University website for the learners prepared by the Audio Visual Production & Research Centre (AVPRC), hosting course material and syllabi for learners.

Enabling the learners to download hall tickets for the examinations and marks memos after the examination.

On-screen evaluation for theory exams. Valuation is digitalized for all the courses where examiners evaluate answer scripts digitally on screen and assign the marks securely. All the answer scripts are scanned for permanent storage and processing.

Learners are allowed to communicate their grievances through the University Mobile App and the University website.

### **3. Network (Intranet & Internet) Use Policy**

Network connectivity provided throughout the University referred to hereafter as "the Network", is either through an authenticated network access connection or a Virtual Private Network (VPN) connection, governed under the University IT Policy. The Communication & Information Services (Computer Centre) is responsible for the ongoing maintenance and support of the Network, excluding local applications. Problems within the University's network should be reported to Computer Centre.

## A. IP Address Allocation

Any computer (PC/Server) that is connected to the university network, should have an IP address assigned by the Computer Centre. Following a systematic approach, the range of IP addresses will be allocated to each user based on VLAN. Majorly each branch is assigned with VLAN, for example, the Academic branch has VLAN-5, Examination Branch has VLAN-6 (Confidential). So, any computer connected to the network from that VLAN will be allocated an IP address only from that Address pool. Further, each network port in the room from where a computer will be connected will have a binding internally with an IP address, so that no other person can use that IP address without authorization from any other location.

As and when a new computer is installed in any location, the concerned user can download the application form available for IP address allocation and fill it up and get the IP address from the Computer Centre. An IP address allocated for a particular computer system should not be used on any other computer, even if the other computer belongs to the same individual and is connected to the same port. IP addresses are given to the computers but not to the ports. The IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose. The computer also should be obtained separately by filling up a requisition form.

**The Computer Centre configures DHCP and Proxy Service for all the users to identify user activity on the network and internet.**

**B.** Use of any computer at the end-user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered an absolute violation of the IP address



allocation policy of the university. Similarly, the configuration of proxy servers should also be avoided, as it may interfere with the service run by the INTERNET UNIT. Even the configuration of any computer with an additional network interface card and connecting another computer to it is considered a proxy/DHCP configuration. Non-compliance with the IP address allocation policy will result in disconnecting the port from such a computer connected to the network. The connection will be restored after receiving written assurance of compliance from the concerned department/user.

### **C. Wireless Local Area Networks**

- i) This policy applies, in its entirety, to departments, or divisions of wireless local area networks. In addition to the requirements of this policy, departments or divisions must register each wireless access point with the Computer Centre including Point of Contact information.
- ii) Departments or divisions must inform the Computer Centre of the use of radio spectrum, before implementation of wireless local area networks
- iii) Departments or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.
- iv) If an individual Department wants to have an inter-building wireless network, before installation of such a network, it should obtain permission from the University authorities, for which the application may be routed through the In-Charge, Computer Centre.

### **4. Email Account Use Policy**

To increase the efficient distribution of critical information to all Faculty, staff, and the University's administrators, it is recommended to utilize the official emails, for formal University communication and academic & other official purposes. The University is using an email facility provided by the National Informatics Centre (NIC) instead of maintaining its email service, as this reduces the burden on the University and provides more security for emails. Email access is by URL: email.gov.in. The University has provided designation-based email ids and name-based email ids with the university domain name user@braou.ac.in.

- i) The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- ii) Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail the 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 the generation of threatening, harassing, abusive, obscene, or fraudulent messages/images.

- iii) Users should keep the mailbox used space within about 80% of the usage threshold, as a 'mailbox full' or 'mailbox almost full' situation will result in the bouncing of mail, especially when incoming mail contains large attachments.
- iv) Users should not open any mail or attachment that is from an unknown and suspicious source. Even if it is from a known source, if it contains any attachment that is suspicious or looks dubious, the user should get confirmation from the sender about its authenticity before opening it. This is very much essential for the security of the user's computer, as such messages may contain viruses that have the potential to damage the valuable information on one's computer.
- v) Users should download KAVACH App on their computer or mobile so that they can use it permanently, to ensure more secure email access. KAVACH is a double authentication system introduced by the NIC.
- vi) Users should not share their email accounts with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- vii) Users should open/use official emails regularly to avoid blocking/expiry problems. If the email is not accessed for more than six months, the email id automatically expires.
- viii) Impersonating the email account of others will be taken as a serious offense under the University IT security policy.

## 5. Website Hosting Policy

### i) Official website

This is the main website of the University registered in ERNET India for hosting University's official information including University acts, profile, governing body details, etc.

Branches, Departments, Learner Support Centers details, Teachers/Employees/ Student related pages on BRAOU's official Web page

As of date, the University's Computer Centre is responsible for maintaining the official website of the University viz., <http://www.braou.ac.in>

The Computer Centre updates the University website by getting official information from concerned branches. For website content verification and content approval, the University formed a committee called the **"Website Maintenance Committee"**

### ii) Web portal for Learner Support Services

The University has a separate Web portal for online services for the learners. As of date, the university's Computer Centre is responsible for maintaining the official website of the University viz., <https://www.braouonline.in>



### iii) Web portal for e-learning

Web pages for e-Learning are authored as a result of the Teaching/Learning Process. Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Website, linked through the concerned department's pages. As of date, the University's Centre for Online Learning is responsible for maintaining the official website of the university for online learning viz., <https://www.elearning.braou.ac.in>

## 6. University Data Use Policy

This Policy relates to the databases maintained by the University administration under the University's online services. Data is a vital University resource for providing useful information. Its use must be protected even when the data may not be confidential.

- A. **Database Ownership:** BRAOU is the data owner of all the institutional data generated in the University.
- B. **Custodians of Data:** Individual Sections or departments generate portions of data that constitute the University's database. They may have custodianship responsibilities for portions of that data.
- C. **Data Administrators:** Data administration activities outlined may be delegated to some of the officers in that department by the Data Custodian.
- D. **MIS Components:** For e-Governance, the Management Information System requirements of the University may broadly be divided into seven categories. These are:  
MANPOWER INFORMATION MANAGEMENT SYSTEM (MIMS)
  - STUDENTS INFORMATION MANAGEMENT SYSTEM (SIMS)



- FINANCIAL INFORMATION MANAGEMENT SYSTEM (FIMS)
- PHYSICAL RESOURCES INFORMATION MANAGEMENT SYSTEM (PRIMS)
- PROJECT INFORMATION MONITORING SYSTEM (PIMS)
- LIBRARY INFORMATION MANAGEMENT SYSTEM (LIMS)
- DOCUMENT MANAGEMENT AND INFORMATION RETRIEVAL SYSTEM (DMIRS)

Here are some general policy guidelines and parameters for Sections, Departments, and Administrative Unit data users:

- i) The university's data policies do not allow for the distribution of data that is identifiable to a person outside the university.
- ii) Data from the University's Database including data collected by departments or individual faculty and staff are only for the internal purposes of the University.
- iii) One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the University will make the information and data available, subject to one's responsibilities/rights.
- iv) Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys, and other requests for data. All such requests are to be forwarded to the Office of the University Registrar.
- v) Requests for information from any courts, attorneys, etc. are to be handled by the Registrar's Office of the University and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the University Registrar for a response.
- vi) At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation, or other purposes. This includes organizations and companies which may be acting as agents for the University or its departments.
- vii) All reports for UGC, MHRD, and other government agencies will be prepared/compiled and submitted by the Registrar, Directors, Controller of Examinations, and Finance officer of the University.
- viii) The University Staff updates/modifies/deletes student records with proper approvals and authorization. Any modification or update on database records must be verified and approved by the designated authority
- ix) Data backup is the daily activity of the University Computer Center. At present, Computer Center staff is maintaining a manual backup of the database. Every day a backup copy of complete data is maintained with the date and time for proper storage and the latest

copy for retrieval. In the case of other information like student photos, only day-wise backup in the folder (incremental backup) is maintained.

- x) Maintenance of logs: The University is maintaining the log details for information security and data protection for every application and transaction.
- xi) Tampering with the database by the department or individual user comes under a violation of IT policy. Tampering includes, but is not limited to :
  - Modifying/deleting the data items or software components by using illegal access methods.
  - Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
  - Causing a database or hardware or system software to crash, thereby destroying the whole or part of the database deliberately with ulterior motives by any individual.
  - Trying to break the security of the Database servers.

Such data tampering actions by University members or outside members will result in disciplinary action against the offender by the University authorities. If the matter involves illegal actions, law enforcement agencies may be involved.

- xii) Summary of Punishments for Improper Behavior Blocking Resources:
  - a) Playing games using University's computing and communication resources, unless they are related to academic/research activities.
  - b) Locking the screen of machines belonging to the university.
  - c) Sending junk/fake mail to all the users.
  - d) Forwarding chain emails.

The minimum punishment is a suspension of computer access facilities for two weeks. Additionally, fines may also be imposed.

### **Misusing Facility**

- a) Unnecessary downloads from the Internet.
- b) Giving accounts to other persons, sometimes outsiders.
- c) Storing pornographic material on the disk.
- d) Viewing pornographic material on terminals.
- e) Using a personal account to do outside(non-institute) work for which the individual is paid.

**The minimum** punishment is suspension of access to facilities for six months and such cases are to be sent to concerned authorities for disciplinary action.

**Security-related misuse:**

- a) Breaking the security of the systems
- b) Trying to capture the password of other users
- c) Damaging/gaining access to the data of other users

*This kind of abuse is taken most seriously. Anyone found involved in these activities will have access denied to their computer for one year. The cases will be sent to concerned authorities for necessary disciplinary action.*

**Anonymous mail forwarding**

*Anonymous mail forwarding is grounds for the removal of campus network privileges for not less than one full semester.*

**Software-related Misuse:**

**i) Using any kind of software without the correct license**

*This kind of abuse is taken most seriously. Anyone found involved in such activity will be denied access to facilities and will be liable for direct action from the software provider-manufacture company for any breach of licensing and the University bears no responsibility.*

**ii) Downloading/Distributing copyrighted materials**

*Users found to be misusing network connections for the download/distribution of copyrighted materials will have their privileges revoked for not less than one year and are subject to disciplinary action.*

**Network-related Misuse:**

- i) Using an IP address to which one is not assigned or using an Ethernet hardware address that is different from the one registered with the Computer Centre.
- ii) No routers are permitted to be attached to any portion of the campus network without the approval of the Campus Network Facility.
- iii) Domain Name Violation

*Systems violating domain name guidelines will be immediately disconnected from the campus network for not less than one semester.*

### **Monitoring and Review Committee**

1. In charge, Centre for Online Learning
2. Systems Engineer
3. Director, EMR&RC
4. Dean, Faculty of Sciences
5. Head, Department of Mathematics

★ ★ ★