IT POLICY & GUIDELINES

हरकोर्ट बटलर प्राविधिक विश्वविद्यालय
कानपुर

श्रम एव परं तपः

Harcourt Butler Technical University
Nawabganj, Kanpur, Uttar Pradesh– 208002

1. Introduction

Harcourt Butler Technical University (HBTU) Kanpur provides IT resources to support the educational, instructional, research, and administrative activities of the University and to enhance the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work. These resources help them to remain well informed and carry out their functions in an efficient and effective manner.

This document establishes specific requirements for the use of all IT resources at HBTU. This policy applies to all users of computing resources owned or managed by HBTU. Individuals covered by the policy include (but are not limited to) faculty and visiting faculty, staff, students, alumni, guests, external individuals, departments, offices and any other entity which fall under the management of Harcourt Butler Technical University accessing network services via HBTU's computing facilities.

For the purpose of this policy, the term 'IT Resources' includes all university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Misuse of these resources can result in unwanted risk and liabilities for the university. It is, therefore, expected that these resources are used primarily for university related purposes and in a lawful and ethical way.

2. Scope

This policy governs the usage of IT Resources from an end user's perspective. This policy is applicable to all individuals/ users/ entities, who use the IT Resources of HBTU.

3. Objective

The objective of this policy is to ensure proper access to and usage of HBTU's IT resources and prevent their misuse by the users. Use of resources provided by HBTU implies the user's agreement to be governed by this policy.

- University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.

- This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

4. Roles and Responsibilities

The following roles and responsibilities are envisaged from each entity respectively.

1) HBTU shall implement appropriate controls to ensure compliance with this policy by their users. Computer Centre shall be the primary Implementing Agency and shall provide necessary support in this regard.
2) Computer Centre shall ensure resolution of all incidents related to the security aspects of this policy by their users.
3) Use's IT resources for those activities that are consistent with the academic, research and public service mission of the University and are not "Prohibited Activities".
4) All users shall comply to existing national, state and other applicable laws.
5) Abide by existing telecommunications and networking laws and regulations.
6) Follow copyright laws regarding protected commercial software

or intellectual property.

7) It is responsibility of the University Community to know the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. University Community is responsible for exercising good judgment in the use of the University's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

8) As a representative of the community, each individual is expected to respect and uphold the University's good name and reputation in any activities related to use of ICT communications within and outside the university.

9) Competent Authority should ensure proper dissemination of this policy.

5. Privacy and Personal Rights

1) All users of the university's IT resources are expected to respect the privacy and personal rights of others.

2) Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).

3) While the University does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.

4) The university is bound by its End User License Agreement (EULA), respecting certain third party resources; a user is expected to comply with all such agreements when using such resources.

6. Privacy in Email

While every effort is made to ensure the privacy of HBTU email users, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct University business, there may be instances when the University, based on approval from competent authority, reserves and retains the right to access and inspect stored information with the consent of the user.

7. User Compliance

When an individual uses's IT resources, and accepts any University issued computing accounts, it means that the individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep oneself up-to-date on changes in the IT policy of HBTU and adapt to those changes as necessary from time to time.

8. Access to the Network

Access to Internet and Intranet

1) A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the University Campus wide LAN.
2) Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

Filtering and blocking of sites:

1) Computer Centre or any other Implementing Agency (IA) may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.
2) Computer Centre or any other Implementing Agency (IA) may also block content which, in the opinion of the university, is inappropriate or may adversely affect the productivity of the users.

9. Monitoring and Privacy

1) Computer Centre or any other Implementing Agency (IA) shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

2) IA/Nodal Agency, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on University provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.

12. E-mail Access from the University Network

1) E-mail service authorized by HBTU and implemented by the Computer Centre shall only be used for all official correspondence.

13. Access to Social Media Sites from Network

1) Use of social networking sites by users is governed by "Framework and Guidelines for use of Social Media for Government Organizations".

2) User shall comply with all the applicable provisions under the IT Act 2000, while posting any information on social networking sites.

3) User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.

4) User shall report any suspicious incident as soon as possible to the competent authority.

5) User shall always use high security settings on social networking sites.

6) User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.

7) User shall not disclose or use any confidential information obtained in their capacity as an employee of the university.

8) User shall not make any comment or post any material that might otherwise cause damage to HBTU's reputation.

DEPARTMENT OF MECHANICAL ENGINEERING
यांत्रिकी अभियंत्रण विभाग

14. Intellectual Property

Material accessible through the network's and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use HBTU's network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

15. Deactivation

1) In case of any threat to security of systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the IA.

2) Subsequent to such deactivation, the concerned user and the competent authority of the university shall be informed.

16. Review

Future changes in this Policy, as deemed necessary, shall be made by the Technical Committee (ICT) with the approval of the Competent Authority of the university.

17. IT Hardware Installation Policy

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

A. Who is Primary User

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

B. What are End User Computer Systems

Apart from the client PCs used by the users, the university will consider servers not directly administered by Computer Centre, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the

Intranet/Internet though registered with the Computer Centre, are still considered under this policy as "end- users" computers.

C. Warranty & Annual Maintenance Contract

Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer Centre from time to time.

D. Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging, till such instances wherein the UPS is to be left unattended. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

E. Network Connection

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

F. File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

G. Maintenance of Computer Systems provided by the University

For all the computers that were purchased by the university centrally and distributed by the Estate Branch, University Computer Maintenance Cell attached with Computer Centre will attend to the complaints related to any maintenance related problems.

18. Software Installation and Licensing Policy

Any computer purchases made by the individual departments/ projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

A. Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through internet. Checking for updates and updating of the OS should be performed at least once in a week or so.

University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

B. Use of software on Desktop systems

a. Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.

b. Any software installed should be for activities of the university only.

C. Antivirus Software and its updating

Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

D. Backups of Data

Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc.

19. Network (Intranet & Internet) Use Policy

Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection is governed under the University IT Policy. The Computer Centre is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to Computer Centre.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the Computer Centre. Each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

B. Running Network Services on the Servers

a. Individual departments/individuals connecting to the university network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the Computer Centre in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network.

b. Computer Centre takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.

c. Computer Centre will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

d. Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes.

20. Email Account Usage Policy

HBTU provides official email access privileges to its users. In an effort to handle the efficient information dissemination among the administration, faculty members, staffs and students, it is recommended to avail official email with Harcourt Butler Technical University domain (hbtu.ac.in).

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

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

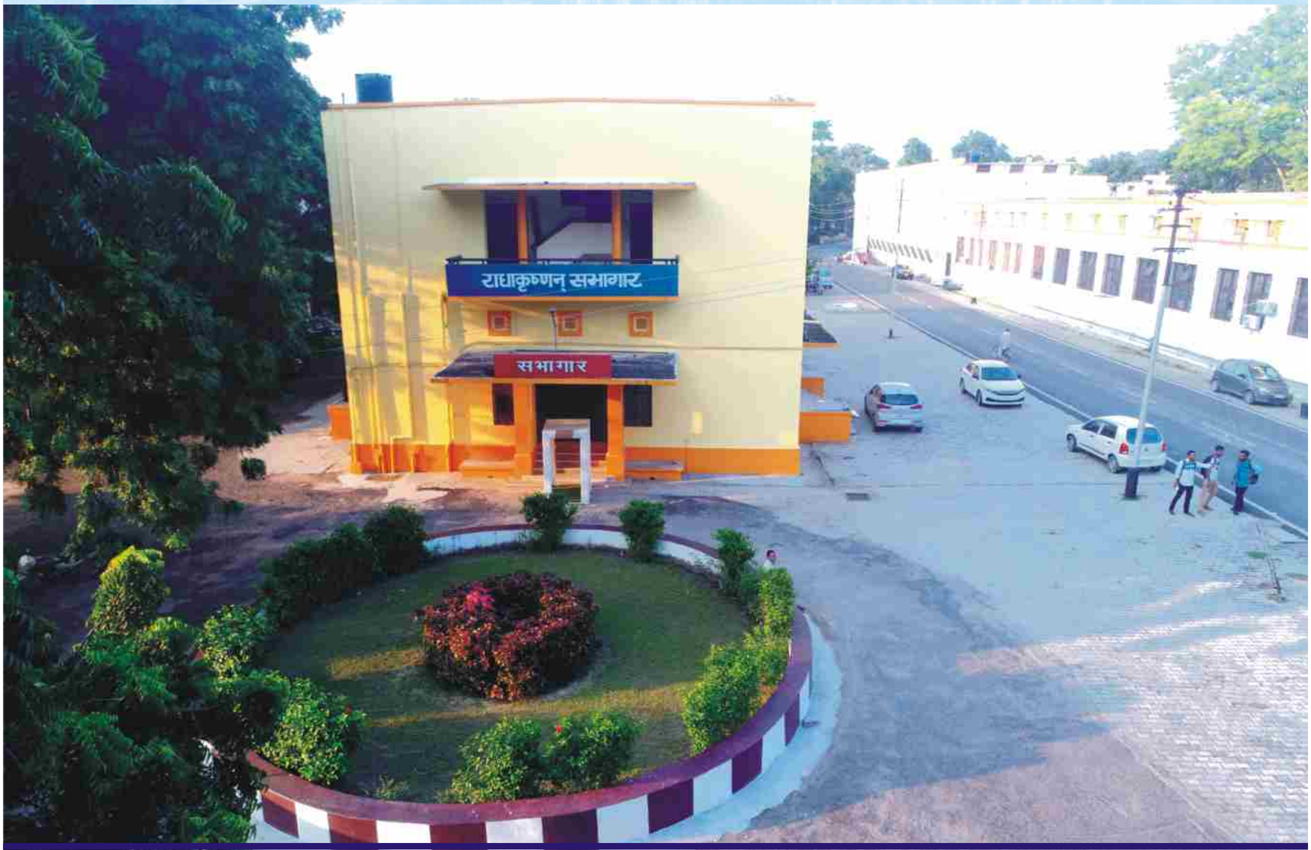
4) Impersonating email account of others will be taken as a serious offence under the IT security policy.

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

6) Students who leave the University having completed a degree program have their @hbtu.ac.in email address deactivated **30 days after losing** their current student status.

7) Employees who leave the University generally have their email address and account deactivated at the time that their employment ends.

8) The above laid down policies are broadly applicable even to the email services that are provided by other service providers such as



Gmail, Hotmail, Yahoo, Rediffmail etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

21. Disposal of ICT equipment

The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the university.

22. Budgetary provisions for ICT

At Harcourt Butler Technical University, use of ICT facilities have been encouraged as it is located in remote area of the country. This has always been a leverage to march shoulder to shoulder with rest of the universities. In view of these scenarios, intends to provide budgetary provisions as follows:

1) Budgetary provisions should be made under recurring grants (OPEX) to maintain all the existing ICT infrastructure for smooth functioning of all the ICT enabled services.
2) Adequate budgetary provisions under capital head (CAPEX) should be kept for upgradation and augmentation of ICT infrastructure.
3) Budgetary provisions under capital grants should also be allocated for implementation of newer ICT solutions from time to time.

23. Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy, the University reserves the right to suspend a user's access to University's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

24. Revisions to Policy

The University reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy, which are available on the website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

Appendix – I: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL ERP & EMAIL ID

(For Faculty & Staff only)

First Name :

Middle Name :

Last Name :

Department/ Branch :

Current Email Address :

Mobile No. :

Note:

1. The filled in form should be submitted after getting duly signed from respective Head of the Department.
2. Information regarding the official Email address created would be sent to your current Email address.
3. An official Email address and ERP credentials would be created within 24hrs. - 48 hrs.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department)

Appendix – II : Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL ERP & EMAIL ID

(For Research Scholars & Students only)

First Name :

Middle Name :

Last Name :

Department/ Branch :

Roll No. :

Duration of Course :

Current Email Address :

Mobile No. :

Admission Year :

Note:

1. The filled in form should be submitted after getting duly signed from respective Head of the Department.
2. Information regarding the official Email address created would be sent to your current Email address.
3. An official Email address and ERP credentials would be created within 24hrs. - 48 hrs.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department)

Harcourt Butler Technical University
मुख्य भवन

हरकोर्ट बटलर प्राविधिक विश्वविद्यालय
नवाबगंज, कानपुर – 208002, उ.प्र., भारत

HARCOURT BUTLER TECHNICAL UNIVERSITY
NAWABGANJ, KANPUR - 208002, U.P., INDIA
(Formerly Harcourt Butler Technological Institute, Kanpur)

Phone : +91-0512-2534001-5, 2533812, website : http://www.hbtu.ac.in, Email : vc@hbtu.ac.in

100 YEARS
1921 - 2021