



हिमाचल प्रदेश केन्द्रीय विश्वविद्यालय
(केन्द्रीय विश्वविद्यालय अधिनियम २००९ के अंतर्गत स्थापित)

धर्मशाला, जिला - कांगड़ा, हिमाचल प्रदेश - १७६२१५

Central University of Himachal Pradesh
(Established under Central Universities Act 2009)
Dharamshala, District Kangra, Himachal Pradesh-176215

**POLICY FOR THE IMPLEMENTATION AND APPLICATION OF MAINTENANCE
PROCEDURE FOR ALL ASSETS OF IT INFRASTRUCTURE NATURE IN
ACADEMIC AND ADMINISTRATIVE AFFAIRS OF THE UNIVERSITY**

PREAMBLE

The purpose of this policy is to ensure the legitimate and optimal use of IT resources at the university. The aim of the policy is to facilitate the safe, secured, effective, target oriented and lawful use based on spirit of cooperation and sharing. The policy shall cover all Information Technology facilities and services provided by CUHP. It shall regulate the use of ICT resources by all the stakeholders and IT facilities & information resources shall be the property of the University and not of a particular individual, School or Centre.

SCOPE:

Details of all assets of IT infrastructure nature and guarantees/warranties of the respective assets - physical, academic and support infrastructure of the university is maintained in the ASSET REGISTER which is available in the Central Store. Maintenance of the respective IT assets that have University wide application is performed under the aegis of Computer Centre. Computer Centre is responsible to extend their services in all the campuses of the university namely Shahpur Parisar, Shahpur, Dhauladhar Parisar-I & II, VC Secretariat at Dharamshala, Sapt Sindhu Parisar-I and II at Dehra, Hostels at Dharamshala, Kangra and Dehra, VC Residence, Yol through their staff. Maintenance procedure which is carried out / adapted includes the following

- Setting out a uniform maintenance and repair procedure for all the devices.
- Ensuring the effective utilization of IT resources for teaching, learning and training.
- Ensuring the replacement/repair of IT assets in a procedural way, and with minimal downtime.

1. HARDWARE SUPPORT:

- a. **Purchase with maximum possible guarantee/warranty:** University prefers to purchase assets of IT infrastructure nature with 3 to 5 years of warranty (whichever is maximum possible).
- b. **Purchases through GeM/ CPP Portal:** Purchase of IT related items are done preferably through GeM portal . In case the desired item(s) are not available on GeM, the respective items may be procured through CPP Portal.
- c. **Repair/ Replacement:**
 - i. In case of non-availability of technical person in the concerned Department , request by the concerned faculty /- staff is made to the Computer Centre through proper channel for their repair/ replacement.
 - ii. For devices under warranty cover of OEM/ Service Provider, the concerned is informed to take corrective action on the receipt of any complaint.
 - iii. For devices out of warranty, staff of the Computer Centre will fix faults if possible. Any faults that can't be rectified by staff of the Computer Centre will be handed over for external servicing.
 - iv. All repairs / replacements shall done as per the university rules and regulation

2. INTERNET SERVICES:

a. Internet Leased Line /P2P Circuit and it's usage:

It is expected that all staff members will use the IT- resources for the purpose in which they are intended to, in a responsible, ethical and lawful manner. In the course of performing their duties, CU Himachal staff members have access to a wide range of confidential information about students, staff and the Institution in general. Information is expected to be accessed only for the purpose of fulfilling job duties. Such information accessed would not be shared or used either internally or externally for any purpose other than its intended use.

The Institution has NKN leased line connection of 1 Gbps as primary link at Shahpur and is further distributed via P2P Circuit of 200 Mbps bandwidth between Shahpur-Dharamshala, 100 Mbps bandwidth between Shahpur-Dehra for sharing of centralized facilities /services . University has three hostels located at different locations Girls Hostel, Shamnagar, Boys Hostel Kachyari, Kangra and Girls Hostel Dehra . All these hostels are connected through 4 Mbps, 10 Mbps Internet Leased Lines (ILLs) and three nos. of FTTH connections respectively. One internet leased line of 16 Mbps bandwidth from BSNL is taken as backup for VC Secretariat, Dharamshala. The entire network is secured externally through firewalls. The internal network is monitored by suitable policies on the firewall. The present wireless network is supervised and controlled by M/s Railtel Corporation of India Ltd. and the present wired network is supervised and controlled by Computer Centre.

Traffic monitoring and intrusion preventions are being carried out time to time or as per the directions of the Ministry by applying suitable policies, filtering of certain IP addresses/URLs. All equipments are protected with UPS to avoid loss of data in case of power failure.

3. ADVANCE BILLING AND BILLING CLEARANCE PROCESS

- a. Computer Centre received quarterly advance billing for 1 Gbps NKN, and yearly advance billing of P2P circuits/ILLs for internet services.
- b. All the concerned bills/matters are placed before the IT/Technical Infrastructure Development Committee for their recommendation(s) and suggestion(s).
- c. Minutes of Meeting of the concerned bill(s)/matter is placed before the Competent Authority for their approval.

4. WEBSITE MANAGEMENT:

Computer Centre maintains the website in association with INFLIBNET for making necessary updations, uploading of notices, circulars, office orders, advertisements, results, timetables, faculty profiles, etc. required or received time to time.

5. TENDERING PROCESS :

- a. Computer Centre prepares the Tenders of all assets of IT infrastructure nature in consultation with Engineering Department whenever required.
- b. After the creation of Tender, same is placed before the Tender Evaluation Committee for their recommendations and suggestions.
- c. Minutes of Meeting of the Tender Evaluation Committee is placed before the Competent Authority for their approval so that same may be sent to Central Purchase Officer (CPO) for the publishing of e-tender on the CPP Portal.

6. STAFF DETAILS: Computer Centre has following Staff members :

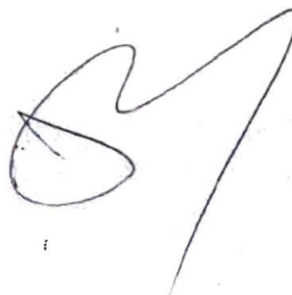
Sr. No.	Name	Designation
1	Prof. Pradeep Nair	Honorary Director, Computer Centre
2	Sh. Girish Sharma	Systems Analyst
3	Sh. Vicky Bhardwaj	STA
4	Sh. Ajay Kumar	STA(Computer) .
5	Sh. Rohit Dhiman	Lab Assistant
6	Sh. Sudhakar Rattan	Lab Attendant

7. FACILITIES:

a. Wi-Fi Facility:

- i. Computer Centre has a predefined template for creation of Wi-Fi accounts of Students/ Employees.
- ii. The primary methods used to authenticate users of the University Wi-Fi resources are User IDs and passwords. Unauthorized access to e-resources or any restricted information found within them are prevented by this primary method.
- iii. It is expected that all users will not share their passwords with any other person and would protect them from disclosure especially with student community, keep changing them regularly, use salted passwords and also monitor usage of respective account through self-care.
- iv. Staff of Computer Centre provides assistance to the end user in the event of lost of password or any suspicious activity.
- v. Each Wi-Fi account is given a monthly quota of 10 GB data and speed upto 20 Mbps.
- vi. University has MoU with Railtel for providing and maintenance of Wi-Fi infrastructure/services in the University.

- b. Institutional Email facility:**
- i. University has subscribed to domain based (hpcu.ac.in) free educational email service of Google (G- Suite for Education) and cuhimachal.ac.in domain based paid email services from ERNET India, are used for official communication.
 - ii. Official email accounts of Staff and RD scholars are created upon receipt of request through proper channel and in a predefined format.
- c. Video Conferencing:**
- i. University has hardware based Video conferencing unit and Video conferencing cameras for the conduct of Online meeting/Interview/ Seminars etc.
- d. Web Conferencing Software :** University has acquired 5 WebEx accounts from I-STEM which has all the features(like recording/broadcasting/support upto 1000 members, etc.) are allotted to each Campus Director for the conduct of Online meeting/Interview /Seminars etc. in their respective campuses on booking basis.
- e. Bulk Email and SMS:** University is registered/subscribed to the use of bulk email and SMS facility with SAMARTH and ERNET.
- f. ERP Portal:** University is given SAMARTH ERP Portal by MoE at no cost. No. of modules are available in the SAMARTH for their implementation in the University. No. of modules of SAMARTH ERP portal has been rolled out in the university like Employee management, Leave Management, Payroll Management, Programme Management, Academics management, student life cycle, Admissions management, Recruitment management, RTI management, Inventory management, grievance redressal, miscellaneous fees portal, etc. Support for the Hands-on training/configuration/ requirement of any feature in the SAMARTH modules, documentation, problem redressal by SAMARTH team is available readily for immediate solution.
- g. IT Service Help Desk Module:-** Computer Centre start using the IT Service Help Desk module of SAMARTH ERP Portal. This module offers the facility of ticket no. generation/ allotment of work to any Staff for their subsequent resolution.
- h. Technical HelpDesk:** - Computer Centre also handle the various technical queries during admission process, semester fee collection, etc. In this regard, one technical helpdesk email-id i.e technical@hpcu.ac.in is used to fullfill this purpose.
- i. IT Training:-** Computer Centre give training to the Students/ Department volunteer to conduct online/offline seminar
- j. Digital EPABX System:-** University has installed digital EPABX of make Matrix and model Eternity 6S and 16S two in nos. at Shahpur Parisar, Shahpur. It supports 64 connections for intercom purposes. This facility is under comprehensive AMC through service provider.



List of Works executed by Computer Centre				
Sr.No.	Assets of IT nature	Under warranty/subscription	Under Annual Maintenance Contract	Service on Call Basis
1	Desktop Maintenance purchased in year 2011 To 2015	No	No	Yes
2	Printers Maintenance purchased in year 2011 To 2015	No	No	Yes
3	EPABX Telephone Exchange System maintenance from 2011	No	Yes	Yes (Free of cost)
4	Desktop Maintenance purchased in year 2022	Yes	Yes, with part replacement	No
5	Printers Maintenance purchased in year 2022	Yes	Yes, with part replacement	No
6	Maintenance of Network Switches, router, any other network accessories/ Services	No	No	Yes
7	Institutional Email Facility	yes	yes	No
8	Web Conferencing Software	Yes	No	No
9	Bulk Email and SMS Facility	Yes	Yes	No
10	Video Conferencing Cameras	Yes	Yes	No
11	Wi-Fi provisioning	Yes	Yes	No
12	University Website	Yes	Yes	No
13	SAMARTH ERP Portal	Yes	Yes, at no cost	No





Central University of Himachal Pradesh
(Established under Central Universities Act 2009)
Dharamshala, District Kangra,
Himachal Pradesh-176215

**POLICY FOR THE IMPLEMENTATION AND APPLICATION OF INFORMATION
TECHNOLOGY IN ACADEMIC AND ADMINISTRATIVE AFFAIRS OF THE
UNIVERSITY**

PREAMBLE

The purpose of this policy is to ensure the legitimate and optimal use of IT resources at the university. The aim of the policy is to facilitate the safe, secured, effective, target oriented and lawful use based on spirit of cooperation and sharing. The policy shall cover all Information Technology facilities and services provided by CUHP. It shall regulate the use of ICT resources by all the stakeholders and IT facilities & information resources shall be the property of the University and not of a particular individual, School or Centre.

SCOPE

This policy shall be applicable for the use of information, electronic devices, computing devices, and network resources of the university. All students, employees, consultants, and other workers at university are responsible for exercising rational judgment regarding appropriate and judicious use of ICT infrastructure in accordance with the following:

- IT Act 2000 including all subsequent Amendments
- E-mail Policy of the Government of India
- Any other policy or guidelines issued by the Government of India from time to time.

Note In addition to above, the university can also devise guidelines for the expansion and use of ICT infrastructure. Such guidelines shall be open for amendments, as and when required.

DATE OF COMMENCEMENT

This policy shall be brought into force from the date of its approval by the statutory bodies of the University.

THE CLAUSES FOR IMPLEMENTATION AND APPLICATION

The clauses are defined briefly within the given context. The expression defined hereinafter shall be construed in following sense:

➤ ***The IT Resources***

The expression IT resource shall include the computer equipment/s, portable and mobile devices, and facilities including the network-internet and intra-net, wireless networks, external storage devices, peripherals like printers and scanners and the software associated therewith and available at any point of time along with the information and data generated for official purpose and all electronic information and communications contained on the network.

➤ ***The Network Resources***

It shall include any electronic/electrical and/or mechanical devices connected to computer network of the university.

➤ ***The Users***

It shall include all students, employees, consultants, and any other person permitted by the Competent Authority for using IT Resources/facilities at the university.

➤ ***Malicious Program***

It includes software that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious codes.

➤ ***Disruption***

It means a circumstance or event that interrupts or prevents the correct operation of system services and functions.

➤ ***Blog***

A discussion or informational site published on the World Wide Web.

➤ ***Competent Authority***

The expression in reference of Section 3 shall stand for statutory body and for section 4.3, it shall be any official designated for the above-said purpose.

- ***Proprietary Information*** It shall include any data, information that has been the part of official assignment and a password of resource, if any.

THE MODALITIES FOR GENERAL USE, ACCESS TO NETWORK AND OWNERSHIP

The proprietary information of the University stored on electronic and computing devices whether owned or leased by the university, the employees, and students or a third party remains the sole property of Central University of Himachal Pradesh.

The users of IT facilities and services of university shall be responsible to promptly report the theft, loss or unauthorized disclosure of the University's proprietary information.

The users shall access, use or share CUHP proprietary information only to the extent it is authorized and necessary to complete the assigned job related responsibilities.

For connecting to CUHP wireless, the user shall ensure the following:

- (a) A user shall register the access device and obtain one-time approval from the concerned Department and submit undertaking, before connecting the access device to the wireless network.

(b) Wireless client systems and wireless devices shall not be allowed to connect to the wireless access points or remote network without due authentication.

(c) To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

(d) The users shall be allowed to remotely access the services and resources of the University by adhering to the procedure to be notified and specified by the competent authority from time to time.

❖ *Filtering and Blocking of Sites*

1. The university, through its Competent Authority may block content on the Internet by issuing a circular, which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or policy of the University or which may pose a security threat to the network or undermine the interests of the university.

2. The university may also block content which, in the opinion of the Competent Authority, is inappropriate or may adversely affect the productivity of the users.

❖ *Security and Password*

1. All IT resources shall be secured by strong password including document as well as equipment password. The password should include a combination of lowercase & uppercase alphabets, numerical and special characters.

2. All computing devices shall be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. The screen must be locked or logged off when the device is unattended.

3. PC shall not be left unattended without logging off and the user shall be responsible for any misuse of such a device by unauthorized access.

4. The users shall exercise utmost caution while opening an e-mail attachments received from unknown senders, which may contain malware.

5. The users shall be responsible for all activity performed with their personal user ID and/or passwords. Permitting any other person to perform any activity with one's user ID and/or

passwords shall be permissible with prior written approval from the competent authority with an undertaking that such a password shall be subsequently changed. These shall be treated as sensitive and confidential information.

6. No official of the University shall require, for whatever purpose, the password of other officials on any kind of questionnaire, in writing or oral, through phone or electronic message service unless permitted by the competent authority in writing with an undertaking that such a password shall be subsequently changed.

7. The users shall refuse all offers by the software to place a cookie on their computer so that they cannot automatically log on the next time when they visit a particular Internet site.

❖ *Electronic Monitoring*

1. The university shall have the right to audit networks and systems at regular intervals, for ensuring compliance of the policy in the case of a specific alleged misconduct or to redress any fault in the functioning of the system. However, this can be done on the prior approval of the competent authority and under intimation to the user.

2. The university or any person authorized on its behalf, 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 the devices under the possession of the university by adopting the following procedure:

(a) The user must be intimated.

(b) If found necessary to access or inspect any device without intimation to its user, it can only be done with the prior approval of the competent authority.

❖ *Unauthorized Access*

Any unauthorized access to any system or its part/s, information or facilities shall be strictly prohibited and invoke disciplinary action. Unacceptable Use Under no circumstances, a user of IT

resources and facilities of the University shall be authorized to engage in any activity that is illegal under Indian or international law.

Following activities shall be prohibited in general. In case, the need arises, select users can be exempted from these restrictions. This list is however not exhaustive, but it provides a basic framework of activities falling into the category of unacceptable usage.

❖ *System and Network Activities*

(a). The 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. b. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the university.

(b) Any infringement of copyright materials including, but not limited to, digitization and sharing of photographs from magazines, books or other copyrighted sources/Movie/Music, and the installation of any copyrighted software for which university or the end user does not have any active license.

(c) Accessing data, a server, an account or any IT equipment for any purpose other than academics, research and official work related to the university.

(d) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.

(e) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

(f) Sharing account password with others or allowing use of account by others including family members while working at home.

(g) Using computing asset of the University to actively engage in procuring or transmitting material that is in violation of sexual harassment/ Human Rights or material considered hostile at the workplace.

- (h) Making fraudulent offers of products, items or services originating from any university account.
- (i) Making statements about warranty, explicitly or implied, unless it is a part of normal job duties.
- (j) Effecting security breaches or disruptions of network communication. Security breaches including, accessing data for which the user is not an intended recipient or logging into a server or account that the user is not authorized to access, unless these duties are within the scope of regular duties. For the purpose of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- (k) Executing any form of network monitoring which shall intercept data not intended for the user's host, unless this activity is a part of the user's normal job responsibility.
- (l) Circumventing user authentication or security of any host, network or account.
- (m) Introducing honeypots, honey nets, or similar technology on the University network.
- (n) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or the Internet/Intranet/Extranet.

❖ *Email and Communication Activities*

While using university IT resources to access and use the Internet, following points are to be adhered to:

1. The users must realize that they represent the University. Whenever users state an affiliation to the University, they must also indicate that "the opinions expressed are my own and not that of the university".
2. E-mail service authorized by the university shall only be used for all official correspondences after the specific notification as to the implementation of this Clause.
3. For personal correspondence, users may use the name-based e-mail id assigned to them on the university authorized e-mail Service.

The following activities are strictly prohibited:

1. Sending unsolicited email messages, including junk mails or other advertising material to individuals who did not specifically request for such materials (email spam).
2. Any form of harassment via email, telephone, whether through language, frequency or size of messages.
3. Unauthorized use or forging of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within the network of the University or from other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CUHP or connected via network of CUHP.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
8. Retiring or the employees being relieved and the students leaving the university shall surrender the mail Id allotted on CUHP domain name or CUHP email server for clearing their No Dues.

❖ *Blogging and Social Media*

In contrast to other traditional media, social media is more interactive, enables one-to-one conversation and facilitates instant response. However, the University is aware of the fact that on such platforms the perception of an official and personal roles and boundaries is often blurred. Therefore, while using social media for official purposes, the following may be kept in mind to smoothen interaction. An official Blogging or access to social media will be regulated by the administrator/ user delegated upon. Limited and occasional use of the systems of CUHP to engage in blogging is acceptable subject to the conditions specified hereinafter.

1. Social Media can be accessed only after office hours. If a user is required to use it for a part of his official assignment or collecting any information during office hours, it can be permitted by the competent authority.

Exception Following shall be exempted from the application of this rule:

- (a) Users or any other official working for the role of Public Relations.
 - (b) Users or any other official working for community outreach under the Community Outreach Programme.
2. There shall be absolute prohibition on the users for making any discriminatory, disparaging, defamatory or harassing comments or bullying while blogging or using social media. The acts, omission or any statement resulting into instigation, abatement to commit any offence, creating communal hatred or apathy shall be strictly prohibited.
 3. No user shall involve oneself in any kind of blogging resulting into compromise with the interests of the university including its employees.
 4. No user shall attribute one's personal statements, opinions or beliefs while using university network while engaged in blogging or accessing social media.
 5. Apart from following all laws of the land pertaining to peace and order as well as the handling and disclosure of copyrighted or export controlled materials, the logos of CUHP and any other CUHP intellectual property shall also not be used in connection with any blogging activity.
 6. Core Values for Users of Blogs and Social Media:
 - (a) Identity: In official communications, user must reveal his identity and his role in the department and publish in the first person. Disclaimer may be used when appropriate.
 - (b) Authority: Users shall not comment and respond unless authorized to do so especially in any of the following matters:
 - i. Recruitment
 - ii. Examinations
 - iii. Tenders
 - iv. Quotations
 - v. Subjudice matter

- vi. Draft Rules, Regulations, Notifications, Circulars
 - vii. Injuring and damaging the reputation of any staff and the student and also the university.
- (c) **Relevance:** The users can comment on issues relevant to their area of specialisation and make relevant and pertinent comments without compromising the interest of the university. This will make conversation productive and help in taking it to its logical conclusion. However, the university shall not take any responsibility for any of such comments and it must be ensured by the user before making any comment or participating in the deliberation that the comments or ideas expressed by her/him are their personal ones, and not of the university.
 - (d) **Professionalism:** The users must be polite, discrete and respectful to all. They shall refrain themselves from making any personal comments for or against any individuals or agencies. They should be careful not to politicize any kind of professional discussions.
 - (e) **Compliance:** The users shall be compliant to relevant rules and regulations. They should not infringe upon IPR.
 - (f) **Privacy:** Personal information about other individuals as well as one's own private and personal details shall not be revealed unless these are meant to be made public.

❖ Dissemination of IT Policy

For dissemination, following measures shall be adopted:

1. Mandatory disclosure of policy on the university Website.
2. Orientation sessions at the time of joining of employees and students to the university.

❖ Disciplinary and Legal Measures

1. Deliberate breach of the provisions contained in this policy statement, shall invoke disciplinary action which may include, in addition to the penalties, denial of access to IT services and facilities offered by the university. On the other hand, if the act is covered with

the meanings and definitions of offences defined under Indian Penal Code, 1860, Information Technology Act, 2000 (with Amendments) and any other allied laws, regulations, the legal proceedings against the person in conflict with policy or offender shall be initiated within the prior written approval of the Competent Authority.

2. Notwithstanding the above, the Competent Authority shall have the Authority to take appropriate action in case any act is not covered under the provisions referred here-in-before if the act or omission affects national interest, interest of the university or proves otherwise offensive.

❖ ***Annual Budget***

On the recommendation of Honorary Director of the Computer Centre, annual budget shall be allocated for the maintenance and up-gradation of the ICT infrastructure for smooth and improved functioning.

❖ ***Power to Revise***

This IT Policy shall be subject to revision by the University from time to time.

❖ **Power to remove difficulty**

If any difficulty arises while implementing this policy, the competent authority can take appropriate decision to remove the same.