Pondicherry University

Information & Communication Technology Policy

Version 1.0

Need

In this era of digital communication, most of the institutes move towards a paperless office where all official proceedings are digitally stored, manipulated and communicated through the internet or intranet. Hence, Information & Communication Technology (ICT) has become the backbone of almost all institutions. Here, ICT refers to the Computer and Communication systems including desktops, laptops, mobile phones, network devices, internet, intranet, Wi Fi, external storage devices, and peripherals like printers, scanners, etc. Misuse of any of these devices might result in colossal risk and liabilities to the institution. Hence there is a need for an ICT policy which lays down the rules, regulations and guidelines stipulating the proper, effective and secure use of these resources for the development of the institution.

SCOPE

Users of Pondicherry University computing, networking and IT facilities are expected to abide by the following rules, which are intended to facilitate fair and secure access/usage of the resources, protect the data and privacy of the work of students, faculty and the administration.

This document also provides guidelines to resolve complaints, in consultation with the higher authorities of the University.

- ICT Hardware Procurement/Maintenance Policy
- ICT System Condemnation Policy
- Website Policy
- E-Mail Usage policy
- Anti-Virus Policy
- ICT/Acceptable Usage Policy
- Network Access Monitoring Policy
- Server Access/Maintenance Policy
- Software Management & Data Usage Privacy Policy

ICT Hardware Procurement/Maintenance Policy

The purpose of this ICT Hardware procurement policy is to provide a framework and guideline for procurement of IT/ICT Hardware by all Schools, Departments and Centres through the funds sanctioned by UGC/MHRD. Also it covers independent bodies like Community College (Lawspet, Mahe & Yanam & Karaikal), HRDC, Distance Education, Hostels, Remote Centres, etc. through funds sanctioned by Pondicherry University.

- Any purchase of ICT hardware or devices by the Department /Centre has to be recommended by the Purchase Committee of the concerned department/centre and submitted to the Purchase Section of the Pondicherry University
- Any purchase related to ICT items one representative from Computer Centre or Department of Computer Science
- The procurement is to be done by the Purchase section following the rules laid down in the Purchase Manual
- All major ICT items shall be purchased with minimum of 3-year onsite comprehensive warranty and wherever required the onsite comprehensive warranty shall be covered upto 5-years from the date of purchase/commissioning
- All ICT items that require operating system software shall be procured either with valid (paid) license or Free and Open Source Software (FOSS)
- The University shall not encourage use of pirated software
- Service Level Agreement (SLA) shall be signed with the Vendor/OEM for proper maintenance support to be provided during the Warranty period soon after issue of the Purchase Order
- A central Asset Registry (software) should account for all the hardware purchased in the University and each department shall also have its own Asset Registry linked to the central registry
- Also hardware purchased as part of the sponsored Projects should be entered into the Asset Registry, since they become the asset of the University once the project gets over
- The Asset Registry should have details of the purchase - Item Name, Quantity, Specifications, Vendor details, PO details, unique Asset ID, date of purchase, Warranty, etc

- On expiry of Warranty, in consultation with the concerned HoD, the Purchase Section shall arrange to cover the hardware items under onsite comprehensive Annual Maintenance Contract (AMC) with the Vendor/Service to ensure continued maintenance support as per SLA
- At any cost, no AMC shall be entered into for items whose stated life or end-of support by the OEM manufacturer has expired. Such items shall be marked for condemnation
- During the valid Warranty/AMC period any complaint/maintenance issue for a particular hardware has to be registered by the User Dept. through the HOD or authorized personnel on the Complaint Management System (CMS)
- The CMS shall be established in consultation with the purchase section and managed by a Service Desk, either established with in-house or outsourced personnel
- The Service Desk shall follow up with the concerned Vendor(s) as per SLA and ensure timely response and resolution of the complaints. Else escalate the issue to the personnel in the escalation matrix
- The Service Desk shall function on 8 hours/day x 5 days/week or 10 x 5 or 8 x 6 to handle the complaints on time
- The Service Desk shall send customised MIS reports to the designated authorities of the University
- Obsolete Hardware or those that could not be repaired /used should be condemned according to the condemnation policy

ICT System Condemnation Policy

(Disposal of ICT, Audio Video and Digital Equipment)

A Condemnation Committee constituted by the University shall, after examination of the items earmarked for condemnation by the user department, shall recommend those items that may be found fit for condemnation.

The Committee shall comprise of members drawn from Computer Centre, concerned user department, Purchase section, Finance Wing, etc

After recommendation of the Committee, these items shall be disposed of by the University Purchase Section following the guidelines issued by the Govt. of India from time to time.

The items ear marked for disposal shall be kept in a secure area until collected by the authorised agency for disposal.

The data/software that may reside in these systems earmarked for condemnation shall be removed by the respective department before disposal. If any leftover information is found, the agency that disposes these items shall provide the University with proof of data erasure or equipment destruction.

The central as well the departmental Asset Registry shall be updated after each condemnation.

Sale of University ICT equipment to individuals is strictly prohibited.

Compliance

All users issued University owned devices must comply with this policy. This includes staff, students, third party contractors and agents. Suppliers who manage IT equipment on behalf of the University must also comply with this policy.

Website Policy

(to be displayed on the website)

Copyright

The Website of Pondicherry University and its contents are subject to copyright protection under the laws of India and, through international treaties, other countries. The copyright in the contents and materials available on this Web-site as a whole is owned by the University. However, the copyright in some contents and materials incorporated within this Web-site may be owned by third parties where so indicated.

No part of the contents or materials available on this Web-site may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of the University. You may view this Web-site and its contents using your Web browser and save an electronic copy, or print out a copy, of parts of this Web site solely for your own information, research or study, provided you (a) do not modify the copy from how it appears in this Web-site

The University's crests and logos should never be removed from pages on which they originally appear. The University's webpages should always appear exactly as posted without variation, unless the prior written approval of the University is obtained.

You must not otherwise exercise the copyright in the whole or any part of the contents and materials in this Web-site for any other purpose except as expressly permitted by any applicable law or with the University's prior written consent.

Trademarks

The logo, crest and name of the University or any of its affiliates are trademarks of the University or its affiliates. The University has policies governing the use of its name, including the names of its schools and programs, and its trademarks. The use, reproduction, copying or redistribution of trademarks without the prior written permission of the University or its affiliates is prohibited. All other trademarks appearing on this Web-site are the marks of their respective owners.

Links from other websites

The University supports and encourages good Netiquette. The University should be informed of links from external websites. However, the University reserves the right to require the removal of any links from external websites to the Pondicherry University website. Deep linking to PU web pages is prohibited - any links created by the user to the University's website

should be text links containing our domain name and which transfer other visitors directly to our homepage. The University requires that the contents of its website should not appear within the frames of others, nor be accompanied in any way by third-party material that may create a false or mistaken impression in the mind of the viewer about the University's affiliation or association with or endorsement of the third party site, frame, or material.

Disclaimer

THE USER ACKNOWLEDGES AND AGREES THAT ALL THE INFORMATION ON THIS WEB-SITE IS PROVIDED "AS IS".

The Pondicherry University ("the University") has used reasonable endeavours to ensure that the information and materials posted on this Web-site are correct at the time of posting. However, the University gives no warranty and accepts no responsibility or liability for the accuracy or the completeness of the information and materials provided here for any purpose whatsoever. No reliance should be made by any user on the information or material so posted; instead, the user should independently verify the accuracy and completeness of the information and/or materials with the originating or authorising faculty, department or other body.

The user acknowledges and agrees that the University shall not be held responsible or liable in any way for any and/or all consequences (including, without limitation, damages for loss of profits, business interruption, or loss of information) that may be incurred by the user as a direct or indirect result of using, or the inability to use, any materials or contents on this Web-site, even if the University has been advised of the possibility of such damages in advance; and no right of action will arise as a result of personal injury or property damage, howsoever arising, sustained as a result of reference to, or reliance upon, any information contained in, or omitted from, this Web-site, whether through neglect or otherwise.

The University reserves the right at any time, from time to time, to make changes to the whole or any part of these terms and/or the services offered on this Web-site as it deems appropriate.

This Web-site may contain links to other World Wide Web sites or resources operated by parties other than the University. Such links are provided as a service for the convenience of the users of this Web-site. As the University has no control over such sites and resources, the user acknowledges and agrees that the University is not responsible nor liable for any content or material on or available from such sites or resources. In providing such links, the University does not in any way, expressly or implicitly, endorse the linked sites or resources or the respective contents thereof. The user further acknowledges and agrees that the University shall not be responsible or liable, whether directly or indirectly, for any damage or loss caused or

sustained by or alleged to be caused or sustained by the user, in connection with the use or reliance on any information or material available on such linked sites or resources.

Personal data protection

If you are only browsing this website or using the Search function, we do not capture data that allows us to identify you individually. This website automatically receives and records information on our server logs from your browser, including your IP address, cookie information, and the page(s) requested. Although user sessions are tracked, the users remain anonymous. Please note that this website may contain links to other websites not maintained by us. Such third party websites are subject to their own data protection and privacy practices and you are encouraged to examine the privacy policies of those websites.

(to be followed by the internal stakeholders of the University)

(http://www.pondiuni.edu.in)

The official web site of Pondicherry University shall be registered under URL http://www.pondiuni.edu.in and is physically hosted in the web server of the Computer Centre on the University premises.

The web server and its contents shall be maintained/updated, secured and supported by the Computer Centre as per the guidelines issued by the University Administration.

Information related to academic, research and administrative functions of the University collected from duly authorized various units of the University shall be hosted on the web site and regularly updated from time to time by the Webmaster in the Computer Centre.

Information to be published on the web site by the internal stake holders of the University shall conform to all norms of copy rights protection, gender/religious/community sensitivity, tender/recruitment/RTI, procedures, etc and must be authentic.

All notices related to administration, teaching/research, examinations, extension activities, events, etc received, after due approval, by the Webmaster shall be published on the web site and no individual copy of the notice shall be sent to the individual (employee) except in certain cases as deemed fit by the Administration.

The notices published on the University web site shall be removed from the web server, after three years from the date of publication on the web site, and kept separately under Archives.

User department that wishes to enable a software application, either developed internally or procured by outsourcing, through the University web server shall obtain necessary security audit certificate from competent agencies and then the software can be enabled for access.

E-Mail Usage Policy

Pondicherry University shall offer e-mail services using the domain **@pondiuni.edu.in** and **@pondiuni.ac.in** to its stakeholders either using its own resources or by availing services from other e-mail Service Providers depending upon the requirement, security and availability of resources.

Any employee (other than outsourced daily wages personnel), students, scholars, long term visiting faculty, others as deemed fit by the Administration from time to time may get Pondicherry University email account created for official use.

- The email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin
- Users who receive any emails with this content from any University employee should report the matter to their supervisor immediately
- Using a reasonable amount of University resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email
- Sending chain letters or joke emails from University email account is prohibited
- Virus or other malware warnings and mass mailings from the University users shall be approved by the competent authority
- These restrictions also apply to the forwarding of mail received by an user to others
- Users can use their favourite email client–Thunderbird, Outlook, Outlook Express, Apple mail, etc
- It is advisable not to use this email system for personal/private correspondences as the University may monitor messages without prior notice
- The University is not obliged to monitor email messages.
- Any user found to have violated this policy may be subject to disciplinary action as per the relevant IT Act or Cyber Laws of Govt. of India

Anti-Virus Policy

- All the Desktop/Laptop/ Workstation computers procured by the University shall have licensed standard Anti-Virus (AV) software installed properly with automatic updation at scheduled time intervals
- The Computer Centre shall guide and monitor the overall protection against viruses and other threats and recommend both end-point and Gateway AV software tools for procurement and installation
- The Computer Centre shall also install Gateway Anti-virus software on the Campus Network
- The concerned Deans/Heads/Section Heads are responsible to create procedures that ensure anti-virus software is installed in their respective units and run at regular intervals
- Timely renewal of the annual AV license and their updation to be ensured by the Purchase section and Computer Centre
- Virus-infected computers must be removed from the network until they are cleared of virus
- Any activities with the intention to create and/or distribute malicious programs into the University systems/networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.
- Any user found to have violated this policy may be subject to disciplinary action as per relevant IT Act and Cyber laws of Govt. of India

IT/ICT Acceptable Use Policy (Rules & Regulations)

Pondicherry University endeavours to provide all faculty, officers, research scholars, guest faculty, research scientists, students and staff with a modern, fully networked computing and IT environment for academic, research and administrative use.

PU users are expected to abide by the following rules. In case of complaints, appropriate action to be taken will be decided and taken by the person in-charge of the facility in consultation with the authority to be nominated by the Administration.

1. PU with authorized accounts may use the computing and IT facilities for academic & research purposes, official purposes, and for personal purposes so long as such use
    a. Does not violate University IT policy or Government of India Policy or law.
    b. Does not interfere with the performance of academic, administration & research.
    c. Does not result in commercial gain or private profit other than that allowed by the University.
2. Users are expected to respect the privacy of other users and they may not allow any other person to use their password or share their account.
    a. It is the users' responsibility to protect their account from unauthorized use by changing passwords periodically and using passwords that are not easily guessed.
    b. Sharing of passwords for any purpose whatsoever is strictly prohibited.
    c. Users may share the required files through a sharing software with proper access control lists (ACL).
3. Any attempt to circumvent system security, or in any way gain unauthorized access to local or network resources is forbidden.
4. Users may not use another person's computing account, attempt to forge an account identity, or use a false account or e-mail address.
5. Use of the internet for commercial gain or profit is not allowed from an educational site.
6. Downloading and installing of new software has to be done with the explicit consent of the respective facility in-charges.
7. Installation of unlicensed software on PU facilities, or on individual machines connected to the PU network, is strictly prohibited.

8. Setting up of any facility requiring password transmission over clear text is prohibited without TLS/SSL encryption.
9. To the extent possible, users are expected to use only their official email addresses provided by PU for official communications.
    a. It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data.
    b. Chain letters are not allowed. Neither is any form of commercial advertising, or soliciting allowed. Spamming is strictly disallowed.
    c. Subscribing to mailing lists outside the Institute is an individual's responsibility.
    d. Subscribing someone else to any group outside University is illegal.
10. Broadcast of messages to everyone in the system is allowed only for academic purposes and emergencies.
11. Violations of this will result in immediate freezing of user's account for an extended period as determined by the authorities.
12. Shared email accounts for any purpose whatsoever are not allowed.
13. Any special accounts, if need to be set up for conferences and other valid reasons as determined by the institute authorities, must have a single designated user.
14. Recreational downloads and peer-to-peer connections for recreational purposes are banned.
15. To the extent possible, users are expected to connect only to the official Wi Fi network for wireless access.
16. Setting up of unsecured Wi-Fi systems on the University network is prohibited in the Campus.
17. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility.
18. Playing of Games in the laboratories or using University facilities is strictly prohibited.
19. Display of offensive material (either on computer screens or through posters etc.) is strictly disallowed and serious action will be taken against offenders.
20. Violations of policy will be treated as academic misconduct, misdemeanour, or indiscipline as appropriate.
21. Depending upon the nature of the violation, the institute authorities may take an action by issuing a warning through disabling the account.

22. In extreme cases, the account may be completely deleted or sent to the University disciplinary action committee as constituted by the Institute authorities.
23. 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.

Network Access and Monitoring Policy

Policy

The network must be designed and configured to deliver levels of performance, security and reliability suitable for the University's needs, whilst providing a high degree of control over access.

Users of University networks are to be explicitly advised that normal operational network management procedures will include: probing devices to test their security and the monitoring of network traffic to detect operational problems or possible policy violations.

Connecting devices to the network

Ownership of networked devices: Only devices owned by the University, or its recognised partner organisations such as the Student's Union/University Hospitals, may be connected to the "wired" network. Privately owned devices may only be connected to the "wired" network in special circumstances approved by the Head of Department. Privately or University owned laptops/PCs may be connected to the wireless network. All devices whether privately owned, or owned by other organisations, must meet the hardware and software requirements, and their usage must conform to University policies.

Administration of networked devices

Every networked device must be associated with an identifiable and contactable person responsible for its administration. Devices for which the administrator cannot be identified or contacted are liable to be removed from the network.

DHCP Servers

The Computer Centre provides DHCP service in all VLANs of the University to enable automatic IP configuration of clients. Installation of unauthorized DHCP servers, without explicit consent from the Centre, will not be not permitted in any PU VLAN as such DHCP servers can interfere with normal usage.

Wi Fi routers and Access Points (APs)

Installation of unprotected Wi Fi routers

Installation of Wi Fi routers in the University campus will not be permitted without explicit consent from the Computer Centre. All users should use the authorized WI FI SSIDs for Wi Fi access and verify the authenticity of the Wi Fi routers

All Wi Fi routers should have at least WPA2-PSK (pre-shared key with WPA2 encryption) standard security enabled.

The GOI regulation prohibits shared access of Wi Fi resources and mandates Wi Fi access only through a central authentication mechanism. In view of this, 802.1x (WPA2-Enterprise) is the minimum acceptable standard for setting up Wi Fi access

Connecting other ISP networks to PU LAN

It is strictly prohibited to connect other ISP networks (not obtained through the Computer Centre) to the PU Network.

In case it is allowed for research or special operational needs it will be the responsibility of the facility in-charge to completely firewall the external network from the PU Network both for inward and outward connections.

Virtual Private Network (VPN) and Secure SHell (SSH) Access

It is strictly prohibited to setup unauthorized VPN or SSH access facilities for connecting to PU Network from outside without explicit consent from the Computer Centre. The VPN facility, if made available at the Computer Centre, should be used for such purposes.

It is also prohibited to facilitate external access to the Pondicherry University network using any terminal sharing or other similar software. The VPN facility shall be made available to needy faculty, staff and research scholars on the recommendation of their Head/Supervisor.

Access Monitoring

ARP monitoring is to be enabled on all VLANs and all IP address to MAC address mappings will be logged and maintained for a period of three months.

Network Usage monitoring

Usage of PU Network (wired `& wireless) will be monitored on daily/weekly schedule and access usage may incur financial penalties or suspension of privileges.

Residents of Faculty/Staff/Officers on the campus and PU Guests shall be provided access to network (wired or wireless) and internet.

Internet access (wired LAN)

Internet access from the wired LAN will be available and access will be restricted to ftp, http and https protocols through designated ports. All accesses will be logged along with the URL, time of access and uid of the user. The logs will be maintained for a period of three months.

In addition, for specified network ports 802.1X authenticated LAN services may be provided on request where technically feasible. In these authenticated ports, all ports can be opened on request.

Internet access (wireless LAN)

Connecting to the SSIDs will require 802.1x authentication and all wireless network traffic will be encrypted using WPA/WPA2 standards. All authentications will be logged along with time of access, uid of the user, registered DHCP IP address and the MAC address of the accessing device.

All logs will be maintained for a period of minimum three months.

Static IP addresses for inward connections

On special requests static external IP addresses may be allocated to specific servers for access from outside on specific ports. This may be required for designated web servers and other research facilities. In all such cases it will be the responsibility of the facility in-charge to install proper firewall and security measures to ensure that the access is restricted to the specific server and the PU network is completely protected from external accesses.

Unrestricted external access from designated servers

Unrestricted access to internet access may be given from specific servers on request for special research and operational needs. It will be the responsibility of the facility in-charges to ensure that access to such a facility is restricted and the users adhere to the relevant policies of the University.

Access logs are maintained for accesses on all ports as required by GOI regulations

Server Access/Maintenance Policy

1. Policy

a. Ownership and Responsibilities

i. An operational group in the respective Department/Centre/Section that is responsible for system administration must own all internal servers deployed at PU.

ii. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Director/Deans/Heads.

iii. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment.

iv. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Director/Deans/Heads.

v. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System Version
- Main functions and applications, if applicable

vi. Information in the management system must be kept up-to-date.

vii. Configuration changes for production servers must follow the appropriate change management procedures.

viii. All logs will be maintained for a period of three months.

ix. On special requests static external IP addresses may be allocated to specific servers for access from outside on specific ports. This may be required for designated web servers and other research facilities.

x. Unrestricted access to internet access bypassing the proxy servers may be given from specific servers on request for special research and operational needs. It will be the responsibility of the facility in-charges to ensure that

i. access to such a facility is restricted and users do not use such a facility to access the internet bypassing the proxy servers

ii. IT usage policy and privacy policy are strictly adhered to.

iii. Access logs are maintained for accesses on all ports as required.

b. General Configuration Guidelines

i. Operating System (OS) configuration should be in accordance with approved Department/Centre/Section guidelines.

ii. Services and applications that will not be used must be disabled where possible.
iii. Access to services should be logged and/or protected through access-control.
iv. The most recent security patches must be installed on the system as soon as practical.
v. Trust relationships between systems are a security risk, and their use should be avoided.
vi. Do not use a trust relationship when some other method of communication will do.
vii. Always use standard security principles of least required access to perform a function.
viii. Do not use root when a non-privileged account will do.
ix. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH).
x. Servers should be physically located in an access-controlled environment.
xi. Servers are specifically prohibited from operating from uncontrolled cubicle areas

c. Monitoring

i. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs would be kept online for a minimum of 1 year.
    - Daily incremental backups will be retained for at least 1 week.
    - Weekly full backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 3 years.
ii. Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

d. Routine Precautions

a. Only authorized administrators are authorized to login to the mail, web, proxy and other servers.
b. The designated system administrator/operational group receives an email alert whenever such an advice is released by the official maintainers of the software.
c. The software is updated periodically and whenever required.
d. All ports except those necessary for functioning of the servers are blocked (firewalled) both from outside and inside.

e. Standard intrusion detection software is run on the PU network to monitor any change of MAC addresses corresponding to IP addresses of trusted machines. The Systems Manager automatically receives an email alert in such cases.

e. DHCP Server

i. The DHCP service of PU to enable automatic IP configuration of clients.

ii. Installation of unauthorized DHCP servers, without explicit consent from the Computer Centre, will not be permitted in any VLAN as such DHCP servers can interfere with normal usage.

f. Compliance

i. Audits will be performed on a regular basis by authorized organizations within PU.

ii. The Computer Centre group, in accordance with the Audit Policy, will manage audits.

iii. Computer Centre Group will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

iv. Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement

Any employee/user found to have violated this policy may be subject to disciplinary action and as per IT laws of Govt. of India.