Information Processing Unit / Computer Centre

Information Systems Acceptable Usage Policy @ BITS Pilani Campuses

The *INFORMATION PROCESSING CENTRE (IPC) / COMPUTER CENTRE (CC)* at various BITS Pilani campuses provide facilities to support and enhance the educational vision and mission of the university. IPC / CC facilitates access to information Technology (IT) resources, communications networks, IT solutions and services to students, faculties and staffs within the culture of openness, trust, and integrity amongst the user community to carry out their research and academic activities with improved efficiency.

IPC / CC provides full freedom to utilize its infrastructure efficiently. This comes with additional responsibility of not misusing the given freedom and respecting the rights of everyone. IT team is committed to protect itself, students, faculties, and staffs from unethical, illegal, or damaging actions by individuals. While IPC / CC advocates the concept of complete freedom in using IT services, it recommends certain restrictions towards bringing a healthier IT usage environment to meet the aspirations of user's community at large. Any abuse of the facility may have serious implications on the reputation and the standing of the institute and can bring the facility of the institute into disrepute. Such misuse of the facility will not be tolerated.

The campus wide network at each campus offers internet and intranet services to the entire campus community. Gigabit fiber channel with redundancy is implemented in the backbone of the communication channel. The campus network is protected by firewall.

To offer high quality seamless internet experience to each user, each campus has multiple Internet Service Providers (ISPs) each having multiple ISP links. The optical fibre leased lines are used for the internet needs of users residing or mobile at places like hostels, academic buildings, faculty and staff quarters, guest house etc. Wireless access points are available in campus to facilitate wireless network connection.

To improve security and fairness, all campuses use firewall authentication for protected access. It offers protection against worms, viruses, malwares, data loss, identity theft, etc. It also offers wireless security. A UTM account is created for every user (students, faculties and staffs) of the institute on joining. The number of concurrent devices allowed for a student, staff and faculty vary from campus to campus. Restriction on upload / download is imposed per campus basis depending on bandwidth availability and other constraints. The bigger download requirements which are of academic interest can be satisfied by sending a request to { ipchelpdesk@pilani.bits-pilani.ac.in, itsupport@dubai.bits-pilani.ac.in, net@goa.bits-pilani.ac.in, netsupport@hyderabad.bits-pilani.ac.in} for Pilani, Dubai, Goa and Hyderabad campus respectively. All IT resources provided by the institute are subject to monitoring, with cause, as determined through consultation with the BITS Pilani administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources

as well as monitoring traffic content in response to a legal or law enforcement request to do so. The access logs of individual user are collected and are maintained for a year.

IPC / CC creates and manages official e-mail IDs for all students, staffs and faculties using Google's centralized e-mail solutions. An email account in the email solution offers 100 GB of storage space for faculties and 15 GB of storage space for staff and students. This storage space includes file storage, collaboration tools, file sharing, personal web pages, and calendaring.

To improve the resource utilization of IPC / CC with maximum fairness, this document outlines policies to be followed for using BITS Pilani computing systems. Use of computing systems and facilities include any computer, server or network provided, supported or used by any of the BITS Pilani campuses. Use of computer facilities also includes the use of data / programs stored / processed / transmitted using storage media and network. The purpose of this policy is to ensure that all users (faculties, staffs, students and third party) use BITS Pilani computing facilities in an effective, efficient, ethical and lawful manner. This policy applies to all IT resources owned or leased by the institute and to any privately owned equipment connected to the campus network and includes, but is not limited to, computer equipment, software, operating systems, storage media, campus network, and the Internet. The compliance with the policies is necessary for the continued use of users' freedom. Not only should users stick to the use of the facility in accordance with the policy, but also should report any use that is against these policies or the spirit of these policies. Failure to report infractions of the policy shall also be considered as an act of omission in following the policy. Security breaches could result in reporting to disciplinary committee when any individual is indulged in violating the IT policy or rules of the institute and Govt. regulations (IT Act 2000 / 2008 / Amendments in 2012).

1. The users are allowed to access BITS Pilani computing system and network only with their authorization credentials. DO NOT SHARE with or transfer to user id and passwords with others. These facilities are provided only for academic purposes, official institute purposes and other institute sanctioned activities as long as these
   a. Does not violate any law, institute policy or IT act of the Government of India.
   b. Does not interfere with the performance of institute duties or work of an academic nature (as judged by the Vice Chancellor / Campus Director)
   c. Does not result in commercial gain or profit other than that allowed by the institute.

2. Users are responsible for all the internet and intranet accesses happening through their account. It is the users' responsibility to protect their account from unauthorized use by changing passwords periodically and using passwords that are not easily guessed. Sharing of passwords for any purpose whatsoever is strictly prohibited. If a user lost / forgot his/her account password, please reset it at the earliest. Please approach IT support immediately for assistance, if required. It is strongly recommended to change the passwords once in every 15 days. Also, for an improved service delivery over the Internet, users should keep their end device (PC/Laptop/Mobile devices) with latest antivirus, and an up-to-date operating system.

3. Users are responsible for the content especially the shared content in their devices when they connect it to the network. They are responsible for the content stored in the designated workspace allocated to them (example: file storage area, web-pages, stored/archived emails, on Computer Centre or Department machines). Users are responsible for protecting any information used and / or stored on their personal system(s) as well.

4. Users are responsible for all the network traffic generated by their computer. Physically tampering with network connections / equipment(s), connecting additional (personal) network devices like Routers and Switches or making exclusive use of network resources is STRICTLY NOT ALLOWED in hostels and academic buildings. Users are not allowed to set up his/her own Wi-Fi network which is connected to the campus backbone using routers or software like Connectify/Hotspot etc. Users are not permitted to install proxy / torrent download / games download / direct download etc. Users are not allowed to engage in any activity with intent of degrading the performance of the network.

5. Gaining access to BITS Pilani systems for which proper authorization has not been given or attempting to gain more system access or privileges than allocated is STRICTLY NOT ALLOWED. Users are not allowed to deprive an authorized user from accessing BITS Pilani system.

6. Use of network for creating, sending, storing, uploading, accessing, using, soliciting, publishing or linking offensive, obscene, profane or indecent images or material is STRICTLY NOT ALLOWED. Users are not allowed to create, send, store, upload, access, use, solicit, publish or link material likely to cause annoyance, inconvenience, distress, discrimination, sexual harassment, defamation, misrepresentation, misleading to some individuals or cultures based on gender, race, religious beliefs, disability, political conviction, sexual preferences, age or otherwise. Users are not supposed to deal with material that infringes the intellectual property (including copyright) of another person or organization. Users are not allowed to download pirated software or any suspect malware from the internet and spread the same among other users.

7. Users are not allowed to use email services (or mail relays or fake emailers) and other network communication facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. Users are not supposed to involve in sending emails or messages masquerading as another person or to hide the sender's identity. They are not allowed to send CHAIN letters, JUNK emails and should not involve in Spamming, Tunneling, phishing, spoofing, accessing torrents (peer to peer connections) and recreational downloads. Any communications sent by electronic means will be legally binding on the user initiating the communication. The Designated system administrators have limited capability of account management and do not have access to individual mail boxes. However as a part of an investigation of any misdemeanor, the account in question can be accessed / blocked and user can be denied access to the email facility. Such investigations /

access typically require express approval from the Director in case of investigations against a faculty or a staff, or the Dean / Associate Dean of Students, in case of an investigation against a student. The email facility cannot be used for commercial gain or private profit other than that allowed by the Institute.

8. Users are not allowed to do security related misuse which includes attempting to bypass firewalls and access rules in place, breaking security of the systems, trying to capture passwords of other users, Damaging / Gaining access to the data of other users etc. Users are not allowed to setup servers of any kind (examples: web, mail, proxy) that are visible to the world outside BITS Pilani campuses. Users shall not download, install or run security programs or utilities that reveal security weaknesses. Users are not allowed to share information to third party which will allow circumvention of security systems by the third party.

9. Users are not allowed to cause physical damage to computing or networking facility or property of BITS Pilani.

10. Users are not allowed to install personal software for use on BITS Pilani's computer systems except the ones leased to the user. Users are not allowed to download / install unauthorized / pirated software for use on BITS Pilani's computer systems and their personal system when it is connected with BITS Pilani's network.

11. Users shall not make unauthorized copies of copyrighted software and documents, except as permitted by law or by the owner of the copyright. Copyrighted materials belonging to the entities other than BITS Pilani may not, subject to the allowable exemptions, be transmitted by faculties, staffs or students on BITS Pilani mail / internet system. Setting up a file sharing service (within LAN) which violates Intellectual property rights is not allowed. All users obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission of copyright owner or as may be permitted under the appropriate law. Each user shall observe all terms and conditions of the license agreement, under which the license to use any copyrighted work has been obtained.

12. BITS Pilani routinely monitors usage pattern for its internet and intranet services. The reasons for this monitoring are many, including cost analysis / allocation and management of the internet and intranet facilities etc.

13. Users are STRICTLY NOT ALLOWED to indulge in cyber-crime / cyber-vandalism.

IPC / CC cannot enumerate all the cases. Any activity which causes inconvenience to users, depletes the IPC / CC resources, or jeopardizes the security of the systems, amounts to unethical use. The Institute, whenever possible, gives all legitimate users the discretion to determine how to best use the computing resources and facilities within the guidelines of this policy. Users are responsible for their actions, the consequences of those actions, and the consequences of negligent inaction. As such, users whose judgment leads to activities inconsistent with the policy

risk disciplinary action and possible imposition of restrictions to enforce the guidelines of this policy. 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, email, printed notices, or through the news groups.

BITS Pilani may take any breach of this policy as a sign of misconduct by the user and use may be subject to the following:

(A) Verbal warning
(B) Written warning
(C) Withdrawal of access and system privileges in part or whole
(D) Any combination of above

Serious or repeated breaches of this policy can be constructed as serious or gross misconduct and disciplinary actions may include:

(A) Counseling
(B) Dismissal / Semester debarring / Year debarring / Drop Program
(C) Loss of benefits
(D) Legal proceedings in accordance with State and Federal Law
(E) Any combination of the above

USER AGREEMENT

Information Systems Acceptable Usage Agreement

I have received a copy of BITS Pilani's Information Systems Acceptable Usage Policy. I have read the aforementioned document, understood the same and agree to follow all policies that are set forth therein.

I understand that this Acceptable Usage Policy applies to me, and I am aware that violations of this policy may subject me to disciplinary action, up to and including termination from employment / studies and / or any legal action.

I indemnify BITS Pilani, its officers, and other faculties, staffs and students of any damage, harm and liability arising out of breach of this policy by me or due to any negligence on my part.

Furthermore, I understand that this policy and document can be amended at any time by BITS Pilani. I further acknowledge that any changes in future to this policy may be communicated to me through physical or electronic means.

_____   _____

User Signature   Date

_____

Name & PSRN / ID. No.