Policy on ICT Services

Indian Institute of Technology Bhubaneswar

1. Preamble

This document lays down the rules and guidelines for the use of Institute Login, Email, Group Mail (inclusive of Mailing Lists) and ICT Services. The Computer & Information Technology Services Cell (CITSC) of the Institute shall have the overall responsibility for implementation of this policy on behalf of the Institute. CITSC may withdraw these facilities to any USER (authorized Institute User in singular and Users in plural) without prior notice, if deemed necessary by the Institute.

2. General

2.1 CITSC shall be responsible to provide network access, internet connectivity, Wi-Fi access, email service, intranet and web applications, ERP services, telephony, and the Institute may acquire other ICT services as in future.
2.2 The ICT services of the Institute are provided towards academic, administrative and other such allied activities according to the Acts and Statute of the Institute.
2.3 CITSC is empowered to withdraw / suspend / modify the provided services from time to time based on various parameters as defined by the Institute over time.
2.4 Users are expected to use their access to the resources as in 2.2
2.5 User shall use these resources in a responsible manner, respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, state and national laws, and Institute policies and standards in vogue from time to time.
2.6 User is issued Institute login (referred as login or USER ID interalia) and corresponding email ID that provide access to the Institute network, email service and other ICT services.
2.7 Chairman, CITSC is the authorized signatory for implementing any exception to this policy complying with the Institute's requirements.
2.8 Chairman, CITSC may delegate all or any part of the implementation of this Policy to various PICs as may deem fit to carry out routine work.

3. Institute Login (USER ID) and User Types

USER shall be provided an Institute Login (hereafter known as User ID) that enables access to the Institute network, email and other ICT services. Users are classified into various user groups with various levels of access and functionality as detailed below:

3.1 **Group A users** are Institute Faculty and Staff.
3.1.1 User IDs under this group are considered permanent and are active as long as the concerned individual is an employee of the Institute.
3.1.2 In the event of retirement/resignation of the employee from service, the User shall cease to have access to the Institute ICT services but will have the email service active for a period of 1-year. After the 1-year period the User ID along with associated data will be deleted unless an extension is granted.

3.1.3 Extension of additional 1-year increment may be permitted on request by the User and approval of HoS / Centre Head / Section Head and the Chairman, CITSC.

3.2 **Group B** users are all Institute Functionaries such as but not limited to Director, Deputy Director, Registrar, Deputy Registrar, Dean, HOS, PIC, Chairperson, President and Assistant Registrar etc.

3.2.1 Group B user IDs shall be created as per the requirement of the Institute and approval of competent authority. These IDs are perpetual in nature.

3.2.2 Group B users will have access to Institute official email and other ICT services (ERP, Intranet etc.) as per their function but shall not have network access linked to their user IDs. The network access will be through their Group A User ID only.

3.3 **Group C** users are Adjunct Professor (all grades); Visiting Professor (all grades); Emeritus Professor and Post-Doctoral Fellow.

3.3.1 User IDs shall be created at the request of the Head of a particular School / Centre to which the User belongs to.

3.3.2 Group C User IDs are for limited duration and will be active only up to the end of the period of employment / contract. After this period the IDs and data shall be deleted.

3.4 **Group D** users are students (Undergraduate, Postgraduate, Research Scholars) enrolled in full-time academic programs.

3.4.1 User IDs shall be created in the beginning of a semester when the Academic Section sends to CITSC the list of newly enrolled students in various academic programs.

3.4.2 Users shall normally not request for login creation directly.

3.4.3 User shall continue with the same User ID in the event of enrolling in another academic program after completion of the currently enrolled one. Such Users shall also be provided with Group E User IDs. The access to network and ICT services shall however be as per Group D user.

3.5 **Group E** users are Institute Alumni.

3.5.1 After successfully completing the academic program, a Group D User shall be transferred into Group E User without changing the User ID.

3.5.2 Group E users shall not have access to ICT services; however, the email service shall remain active and limited guest network access shall be provided. Primarily, Group E users have access to the various alumni mailing lists.

3.5.3 CITSC may decide to withdraw the email service for Group E or limit the email service to forwarding only, if the need arises.

3.5.4 Group D User IDs are life-time valid. However, the status of the IDs will be checked periodically. After periodic checks, unused IDs and their respective data will be deleted.

3.6 **Group F** users are Project Staff (JFR, SRF, Project Assistant, Project Fellow etc.)

3.6.1 User IDs are created on the request of the PI approved by the Head of the concerned School.

3.6.2 User IDs shall be active till the duration of the concerned project. After this period the IDs and data will be deleted.

3.6.3 In the event of a Group F user becomes a bonafide student or Post-Doctoral Fellow or eligible into any other category of User specified in this Policy, the process for User ID creation in the new category will need to be followed even though the user ID remains unchanged.

3.7 **Group G** users IDs are functional IDs connected to office positions such as Director's Office, Office of the Deputy Director, Dean, Registrar and Office of School/Centre etc.

3.7.1 User IDs shall be created as per requirement of the Institute and approval of the competent authority. The IDs are perpetual.

3.7.2 User IDs shall not have network access linked to these IDs and will be used for Institute official email and other ICT services (ERP, Intranet etc.) as required.

3.8 **Group H** user IDs are functional IDs connected to staff positions such as Network Administrators, IT & Computer Services staff, other staff positions that require special network access, higher band-width limits etc.

3.8.1 User IDs shall be created on request of PIC/HoS/Section Head with appropriate justification and on approval by Chairman, CITSC.

3.8.2 User IDs shall have network access, email and other ICT services as per requirement.

3.9 **Group I** users are Interns, trainees, short-term course participants and other guests of the Institute who require access to Institute network.

3.9.1 User IDs will be created on request by Faculty concerned with approval of Head/Dean (Academic Affairs)/Dean (Continuing Education), as the case may be or any other appropriate competent authority in case of Institute Guests.

3.9.2 Group I users will not have email service or Institute ICT services access but will have limited guest network access. The extant of network access will be decided by CITSC from time to time.

3.9.3 Group I user IDs are for limited duration as per the requirement (not longer than 3 months) and shall strictly be of the kind **guestXYZ,** where XYZ is a number.

3.10 **Group J** users who are Contractual Staff (excluding academic project staff) and Outsourced Staff.

3.10.1 Outsourced staff in general will not be issued a user ID however in special case with the proper justification by the HoS/Centre Head/ PIC/Chairperson/Section Head and approval of competent authority IDs may be issued.

3.10.2 User IDs will be active only during the contract period of the staff. After this period the IDs and data will be deleted.

3.10.3 Group J users' access to Institute network, email service, ICT services will be decided on the merit of individual case.

3.11 **Group K** users are functionaries of Institute authorized non-professional and professional bodies related to the Institute such as: Vice-President Gymkhana etc.

3.11.1 User IDs are created on approval of Chairman, CITSC as per request of the Group A users holding offices in these bodies by approval of competent authority of the Institute.

3.11.2 User IDs will have access to email service only. These IDs shall not normally have network and ICT services access unless specifically approved by the competent authority.

4. Email and Electronic Communications

4.1 Usage

4.1.1 The Institute email ID must be utilized for all users' activities related to the Institute viz. academic, research, consultancy and official matters.

4.1.2 All electronic communication, including email, social networking, chats, and blogs and all other forms must be used in a responsible manner and consistent with other business communications (e.g., official correspondence, etc.).

4.1.3 Group B users must use the functional email ID and not their personal email ID associated with their names for all their function related Institute activities.

4.1.4 Users are required to check their Institute email on a frequent and consistent basis to ensure that they are staying updated with all official communications.

4.1.5 For all Users, email is made available for the purpose of conducting Institute related business, but occasional social/personal use is allowed provided it does not interfere with the Users' duties or Institute business or operations and is in compliance with all Institute policies.

4.1.6 Group D users are permitted email for some personal use, provided it does not harm the image and standing of the Institute.

4.1.7 Users shall not have email auto-forwarded from their Institute email address to another email address. However, Individual emails may be forwarded as per need except when the user is not authorized to distribute the email and its contents without prior permission or authorization.

4.1.8 The Institute shall not be responsible for email sent to users by outside vendors, such as: subscriptions, external mailing lists, social networking, etc.

4.1.9 Institute communications sent via email is the responsibility of the User from whom it is originated.

4.1.10 Users must not employ false identity or mask the identity of an account or computer to send emails.

4.1.11 Users must not rebroadcast / send an email to a third party obtained from another individual that the individual reasonably expects to be confidential.

4.1.12 Users must not send emails that are of a fraudulent, defamatory, harassing, or threatening in nature.

4.1.13 **Users must not involve in any ICT related activity that is in violation of the conduct rules of the Institute.**

4.1.14 Unsolicited email is expressly forbidden.

4.1.15 Viewing, storage or transmission of sexually explicit material, pornography and other illegal material is expressly forbidden.

4.1.16 Users must not send/forward chain emails or spam.

4.2 Junk Mail

4.2.1 Junk mail shall be dealt with at the user's end. (Note: Not all junk mail and malicious software can be centrally blocked/eradicated.)

4.2.2 Users should employ safe Internet security practices. Safe Internet practices include: not visiting fraudulent websites that are included as links in suspicious emails; not forwarding/distributing suspicious email or insecure website links; opening attachments/files included in suspicious emails; etc.

4.3 Email Privacy and Monitoring

4.3.1 Users should not write anything in an email that the User would not be comfortable putting in a written memo. (Note that emails can be stored, copied, printed or forwarded by recipients.)

4.3.2 The Institute reserves the right to monitor the content of all electronic communications. The Institute, if required;

4.3.2.1 has the right to look at emails stored, sent, or received on/across Institute computer systems and networks.

4.3.2.2 has the responsibility and authority to monitor individual email accounts and it determines that this monitoring is necessary for legitimate administrative purposes.

4.3.2.3 has the responsibility and authority to access, review and release electronic information that is transmitted over or stored in Institute systems.

4.3.3 The privacy, security, and authorship of documents and messages stored in and transmitted via network (internal / external) or electronic media cannot be guaranteed.

5. Group Email and Mailing Lists

The Institute has established group email as a means of sending official information to students, faculty members, staff and alumni, as the case may be. To support this objective, the Institute provides various group email IDs and mailing lists.

5.1 Group Email IDs and Mailing lists are powerful tools to disseminate information quickly and effectively. Any information distribution unnecessary to the corresponding list and abuse of facility needs to be brought to the attention of the CITSC and the relevant competent authority.

5.2 Abuse of group mail and mailing lists may result in; banning from list, temporary suspension/permanent removal of Institute login and email ID, disciplinary action and civil and criminal prosecution by Institute or third parties or shall amount to misconduct under Institute Conduct rules.

5.3 The CITSC may block/delete unwanted mails from being posted to the group mail and mailing lists.

5.4 Table 1 below summarizes the various group email and mailing lists, the intended purpose and users of the Institute authorized to send emails on these lists and other details.

S. No.	Group Email / Mailing List (@iitbbs.ac.in)	Target Group	Who can Post	Intended Purpose
1.	faculty	All faculty members	From official functional email IDs (i.e. not their personal email ID) created for the Institute functionaries and offices – Group B and G user IDs only	Conveying Official Information
2.	faculty.xyz	All faculty members of xyz School	Group members and as in Sl. No. 1	Conveying Official Information
3.	staff	All staff members	As in Sl. No. 1	Conveying Official Information
4.	staff.xyz	All staff members of the xyz school	As in Sl. No. 1	Conveying Official Information
5.	deans	All Deans	As in Sl. No. 1	Conveying Official Information

6.	hos	All Heads of Schools & Centers	As in Sl. No. 1	Conveying Official Information
7.	officers	All Class I Officers	As in Sl. No. 1	Conveying Official Information
9.	xyz.section	Staff belonging to correspondi ng xyz section	Group members and as in S. No. 1	Internal information related to working of the particular section
10.	all	All users of the Institute	Director, Deputy Director, Registrar, Chairman CITSC, PIC Website & Administrator CITSC.	Relevant Information related to Internet, Network, and Security etc. Emergency notification approved by competent authority
11.	Various lists of bonafide students	All students belonging to the particular group	Group A, B and G users only.	Relevant Information only. Refer to 4.2 related list abuse.
12.	Various lists of Alumni	All alumni students belonging to the particular group	Director, Dean Alumni Affairs, Coordinator Alumni Affairs, and Alumni Members	Relevant Information Only.

6. Antivirus & Internet Security Software

6.1 All computer systems accessing Institute data and networks must have Antivirus and Internet security software installed, active and configured to run at regular intervals. The software must be current and updated at all times.

6.2 Antivirus and Internet security software will not be routinely provided by CITSC.

6.3 It is the responsibility of the User / School / Centre / Lab / Unit / Section / Department to ensure that the Computing and IT systems are managed and protected and do not pose a threat to the wider Institute network and community.

6.4 Users downloading software from a network or installing software from an USB drive / external-disk / CD-ROM, must ensure the software is free from virus, Trojans, key-loggers and other vulnerabilities etc. before installing/using it.

7. Security

7.1 Users must use strong and secure passwords. It is recommended that Users incorporate a mixture of alphanumeric upper and lower case letters as well as special characters in their passwords. Passwords must be at least eight characters long.

7.2 CITSC monitors **only** the strength of the password and **not** the password itself and may suggest the users to change their password to improve the strength from time to time.

7.3 Users must not give or lend their password to anyone.

7.4 Group B, G and H Users, when temporarily handing-over charge to another Institute member, must change the password and hand-over the temporary charge. Under no circumstance should they disclose the password that they use during normal operations.

7.5 Two-factor authentication is available. All Users are recommended to use this added layer of security service.

7.6 Group B, G and H Users must use 2-factor authentication without fail. (Please note Group B, G and H Users have to update the 2-factor authentication during their temporary hand-over.)

7.7 Users should not write down their passwords or store them in text or other unencrypted files, batch files, automatic login scripts, or in other locations where another can see/copy/misuse passwords.

7.8 If a User finds any fraudulent activity from his / her email account or network access, he / she should immediately inform CITSC.

7.9 Users must not log on to a computer / network with his / her User ID / password and let another person use his / her access.

7.10 User is solely responsible for all activities that take place from his / her account. Unauthorized use of an individual's account due to his / her negligence is also considered computer abuse by the user and is dealt as per 8.1.

7.11 The Institute cannot guarantee the confidentiality of any of the files stored on the Institute systems.

7.12 CITSC recommends the installation of personal firewalls on all Institute owned systems and any individual computer accessing Institute network systems to ensure data integrity and security at the user end.

8. Privacy

8.1 CITSC records information about each network session of the User.

8.2 Information recorded includes the username associated with the session, IP address, mac-id, the login and logout dates and times, and the amount and kind of resources used during the session.

8.3 The information collected if required would be used for legitimate Institute purposes only including addressing issues of law, abuse, security or system management.

8.4 If the Institute learns that system security or system operation has been compromised or it has been used for unauthorized activities, the Institute has the responsibility and authority to review the contents of all computers such as: files,

programs and emails. (Institute computers as well as personally owned computers used in the Institute network.)

9. Installation and Use of Unauthorized Software and Hardware

1. Users are forbidden from use of unauthorized hardware, pirated software, and unauthorized copyrighted materials.
2. Installation and use of hardware / software that disrupts the Institute network and ICT services is not permitted and is considered as a computer abuse and the Institute has the right to take appropriate action.

10. Computer Abuses

10.1 Users may lose their login account, be disconnected from the network, face disciplinary action up to and including termination/suspension, possibly be charged with criminal offenses (either by the Institute or third parties) or have civil/criminal action taken against them based on the severity of the computer abuse(s).

10.2 Following are considered as computer abuses:

10.2.1 Unauthorized access of another person's computer or email account.

10.2.2 Unauthorized access of Institute data or systems.

10.2.3 Misrepresenting either the Institute or individual's role at the Institute to obtain access to data or computer systems.

10.2.4 Using computing resources and network services to access any other computer system (on or off-campus) without authorization.

10.2.5 Disseminating any confidential information unless such dissemination is required by the individual's job at the Institute.

10.2.6 Deleting or copying files from another person's computer account without permission/authorization.

10.2.7 Taking advantage of another user's naiveté to gain access to another user's email account, network access, computer account/login, files etc.

10.2.8 Preventing someone from using their account by changing the password or other tampering.

10.2.9 Sending offensive, harassing or threatening messages or repeated unsolicited email.

10.2.10 Abusing the networks (internal, external, NKN, ISP etc.) to which the Institute belongs.

10.2.11 Use of the computer or network for monetary gain, political purposes or illegal activities.

10.2.12 Illegal use of downloaded copyrighted materials including print, audio, and video

10.2.13 Intentionally writing, producing, generating, copying, propagating or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software unless such action is part of authorized research or testing. (Such software is often referred to as a virus, worm, Trojan horse, or some similar name.)

10.2.14 Illegally distributing copyrighted software, copyrighted material including music, videos, motion pictures etc. within or outside the Institute through any mechanism, electronic or otherwise.

10.2.15 Any activity that interferes with the rights of others.

10.2.16 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Institute or the end user does not have an active license is strictly prohibited.

10.2.17 Revealing your account password to others or allowing use of your account by others.

10.2.18 Using Institute computing asset in procuring or transmitting material that is in violation to workplace laws.

10.2.19 Making fraudulent offers of products, items, or services originating from any Institute account.

10.2.20 Any electronic activity not cited above that is considered illegal by the laws of the Republic of India.

11. Compliance with Institute ICT Policy

11.1 All users must be aware and adhere to the Institute ICT policy. Users must sign a written declaration to this effect before access of Institute ICT services is granted.

11.2 Additionally, in case of an outsourced employee, a non-disclosure agreement is to be signed by the concerned outsourced agency.

Glossary

S. No	Keyword / Term	Description
1.	Users	All Authorized Institute Users. Refer to Section 3 of this document for more details.
2.	Login	Login ID created by CITSC that enables user to login into Institute networks, access Internet and other services including email and ICT services.
3.	Institute Official Email ID	See item 4 below.
4.	Functional Email ID	Also called Institute Official Email ID. Login and email ID given to Institute functionaries such as; Director, Deputy Director, Registrar, Deputy Registrar, Assistant Registrars, PICs, Chairpersons, Offices etc.
5.	Personal Email ID	Institute Email ID based on the name of the user as opposed to the function/designation.
6.	ICT Services / Resources	Computer and IT System Resources of the Institute including all hardware, networking equipment, software, IT services including email, group mail, intranet, ERP and other e-Resources. Resources also include networks (internal and external) that the Institute is part of.
7.	PIC	Professor in Charge
8.	HOS	Head of School
9.	Section Head	Section Head may mean the OSD or Assistant Registrar or Officer in-charge of a particular section (academic, finance & accounts, civil works etc.)
10.	Competent Authority	Means Chairman CITSC or Deputy Director or Director as per context.