Acceptable Usage Policy

Indian Institute of Science, Bangalore

Preamble

The Indian Institute of Science (IISc) is India's premier institute for advanced scientific and technological research and education. The IISc community consists of about 4500 students, 500 faculty members, and more than 2000 non-teaching staff members. Members of this community use the Institute's IT resources to connect to the campus network. The campus network is connected to the Internet via leased circuits from several service providers. In this way email and other Internet services are made available across the campus to all the users.

The purpose of this Acceptable Usage Policy (AUP) is to define acceptable practices for the use of the Institute's IT resources, including networks, systems, software and equipment. These resources are provided to support the academic, research, and administrative activities of the institute. Security – including Confidentiality, Integrity and Availability - of the Institute's information and information systems, along with compliance to legal regulations are of paramount importance. Security incidents or compromises at any single point, such as an individual device or account, can jeopardize the security of the entire network and its resources. Hence, it is crucial that all users who use the Institute's IT resources understand their responsibilities to protect the Institute's operations, research data, intellectual property and reputation.

Scope

This policy applies to all users of the Institute's IT resources, including faculty, students, researchers, staff, contractors, affiliates, and external users with authorized access. It covers all devices, whether owned by the institute or otherwise, that are used to access the Institute's IT resources.

Policy

1. General Guidelines

1. The IISc community should be aware that usage of IT resources issues covered by the Indian IT Act 2000, violation of which is an offense under national law.

2. The IISc campus network and internet access resources are meant for official use arising from the academic activities and administrative responsibilities of the faculty, staff and students of the Institute. Reasonable personal use is permissible so long as the activity is not illegal, complies with all other provisions of this policy and the Information Security Policy of the Institute, does not conflict with academic needs or expectations, and does not result in added cost and/or security breach to the Institute.

3. The IISc community should view the network resources with a sense of ownership and

participation and should actively help to prevent and to interdict any misuse. Procedures laid down, from time to time, regarding the management of network resources, must be understood and followed meticulously by the user community.

4. The IISc Network Management Team reserves the right to scan all information carried by the network for the purpose of detecting and identifying inappropriate use. As such the privacy of information carried by the network is not guaranteed. Such scanning will be done only on approval by a competent authority. This is in accordance with the Indian IT Act 2000.

5. Use strong passwords and multi-factor authentication (where required) to access systems and applications. Sharing of credentials is prohibited.

6. All data must be handled in accordance with the Institute's Information Classification standards, as defined in the Information Security Policy.

7. Users are expected to comply with all applicable laws, regulations, and Institute policies.

8. Guest Wi-Fi accounts are available with the department offices, and can be allocated to department guests after approval from the competent authority in the department.

2. Network Usage

1. The IISc campus network and internet access will not be used for commercial activity, personal advertisement, solicitations, or promotions, such as hosting of commercial websites, or email broadcasts of commercial promotions to the IISc community.

2. As such, non-IISc organizations (such as commercial outlets operating on the IISc campus) will not be connected to the IISc network, and cannot be a part of the IISc domain.

3. Users must not engage in activities that disrupt network services, including excessive bandwidth usage. The downloading or streaming of audio and video files is to be done prudently.

4. Access to sites that are banned under law or that are offensive, harassing, obscene or infringes any copyright is prohibited. This is also an offense under the Indian IT Act 2000.

5. Use of the network to tamper with information on other computers, to deliberately spread harmful programs, to hack into and compromise other systems, or to cause damage of any kind using the internet, is prohibited, and is an offense under the Indian IT Act 2000. The user is liable for any civil losses caused, in addition to criminal prosecution under the Indian IT Act 2000.

6. If a department wishes to set up its own Internet access facility, then it should get in touch with the IISc Network Management Team and ensure that deploying such an access facility does not jeopardize the security of the campus network.

3. Email Usage

1. The email service should be used primarily for official purposes.

2. Since email accumulates over time, the storage in email servers can overflow. Users must, therefore, regularly clean their mailboxes to avoid disruption to email services.

3. Use of the email service to send fraudulent, threatening, anonymous or harassing emails is prohibited.

4. Mass email or messages sent to large groups must be authorized by appropriate channels. Spam, chain emails, and unsolicited messages are prohibited.

5. Confidential or sensitive information must be transmitted securely using encryption or other approved methods.

6. Users should not auto-forward official emails to non-official email services.

7. Users should exercise caution when clicking on email links or replying to emails, and verify the authenticity of the links and the sender of the emails before proceeding.

4. Software Usage

1. Software programs are covered by copyrights and a license is required for their use. Users must ensure that they have either a commercial or public license (as in the case of 'free' and 'open source' software) for any software they install on the systems that they are responsible for.

2. Use and exchange of pirated software over the network is prohibited.

3. The downloading and use of software that is not characterized as public domain or 'free', or does not have a valid commercial license is prohibited.

4. The IISc fraternity must respect the property rights of others by never misusing their assets, intellectual property or trade secrets, including the copying or downloading of unauthorized software, trademarks, copyrighted material or logos. IISc supports the rights of copyright owners and does not tolerate reckless or deliberate copyright infringement.

5. The users must not add unauthorized/unlicensed or pirated software or files to any machine and shall not indulge in any unauthorized copying of copyrighted material including, but not limited to, digitization and distribution or installation of any copyrighted software for which IISc or the end-user does not have an active license.

6. The users shall use only licensed versions of the software and ensure that a valid software license for all software installed on IISc owned computers is maintained. Applications must only be installed from official platform-owner approved sources.

7. User shall also refrain from exporting software, technical information, encryption software or technology, in violation of international or regional export control laws and shall not transmit, distribute, download, copy, cache, host, or otherwise store any information, data, material, or work that infringes the intellectual property rights of others.

8. No user will give software or applications to any outsiders, including clients, visitors, external

students, companies, facility users and others.

9. Any user found guilty of the above acts shall be held personally accountable. Users shall be held liable for expenses, losses and damages resulting to IISc due to such action or inaction of the user.

10. Users must not condone the illegal copying of software under any circumstances. If any usage of unlicensed software is noticed, it should be immediately brought to the notice of Network Management Team by email to networksupport@iisc.ac.in.

11. If any user needs to procure licenses for usage of a software, they should contact DIGITS by email to office.digits@iisc.ac.in.

5. System Protection

1. Users are responsible and accountable for the usage of the systems allocated to them.

2. Users must take adequate measures to prevent network misuse from the computer systems for which they are responsible.

3. Reasonable care should be taken to minimize the vulnerability of systems attached to the campus network. Users must apply appropriate service packs and antivirus and client security solutions in their MS Windows machines, and necessary upgrades and OS patches for other systems.

6. Hosting Information on the IISc Network

1. The hosting of web sites on systems attached to the campus network requires prior permission from the competent authority in the department where the site is hosted.

2. A website hosted on the campus network will be linked to the IISc domain only on approval by the competent authority.

3. The hosting of websites that carry offensive or obscene material is prohibited.

4. Domain name for system attached to the campus network requires approval from the competent authority in the department upon which IISc Network Management Team will allocate domain name.

7. Social media usage

1. Only authorized individuals may represent the Institute in an official capacity on social media platforms or public forums.

2. Personal use of social media must not interfere with professional responsibilities or harm the reputation of the Institute.

3. Content shared on official or personal accounts must not include sensitive or confidential information related to the Institute’s activities or personnel.

4. IISc community members are prohibited from making social media posts that contain defamatory, pornographic, or harassing content, or any material that violates the rights or dignity of others or creates an unfriendly campus environment.

8. Appropriate Use of Electronic Information Resources

The Institute has acquired several commercial information resources (e.g., citation databases, electronic journals, and journal archives) that are connected to the campus network. Further, the Institute subscribes to several such resources available over the internet. These resources are extremely valuable to the academic community, but their use is bound by certain contractual obligations. Users are responsible for having read and understood these contractual terms while accessing these resources over the network. Users can refer to the library website for related policies and instructions available at https://library.iisc.ac.in/access-guidelines.

Compliance and Disciplinary Actions

The IISc community is expected to be aware of the contents of this policy document, and agree to abide by its provisions. This Policy will be publicly posted on the IISc website, and all individuals who use IISc network resources should be made aware of this policy. The Information Security Steering Committee will look into all violations of this Policy, and recommend suitable action.