RCB IT Policy

RCB/IT Policy/2023

United Nations Educational, Scientific and Cultural Organization

Regional Centre for Biotechnology

150 YEARS OF CELEBRATING THE MAHATMA

क्षेत्रीय जैवप्रौद्योगिकी केन्द्र
राष्ट्रीय महत्ता की संस्था एवं वैधानिक संगठन, संसदीय नियम के अंतर्गत
जैवप्रौद्योगिकी विभाग, भारत सरकार द्वारा यूनेस्को के तत्वावधान में स्थापित
REGIONAL CENTRE FOR BIOTECHNOLOGY
An Institution of National Importance and Statutory Organization
Established through an Act of Parliament by Department of Biotechnology, Govt. of India, under the auspices of UNESCO

Azadi Ka Amrit Mahotsav

Digital India

हिन्दी / English

Regional Centre for Biotechnology, Faridabad
IT Policy

Preamble:

Regional Centre for Biotechnology (RCB) is an institution for education, training and research established by the Department of Biotechnology, Govt. of India in the auspices of UNESCO as a Category II Centre. The primary focus of RCB is to provide quality education, training and conduct innovative research at the interface of multiple disciplines to create high quality human resource the interdisciplinary areas of biotechnology in a globally competitive research milieu. The Faculty, Staff and Students of RCB have been allocated desktop systems, which are connected to the campus network. The campus network is connected to the Internet via leased circuits from two different service providers. A user-friendly, web-based email and Internet services are made available across the campus to all the users.

The internet access is an essential, though a limited, shared and expensive resource, and can easily be congested by uncontrolled and arbitrary usage. The academic users expect a certain level of performance and availability. Further, certain legal issues arise when connecting the private network of a national institute to the public Internet. It is because of such reasons that it has been felt necessary to develop an IT infrastructure/Internet usage policy for the institute and users to follow the same.

General Guidelines for the RCB community:

1. Many network usage issues are covered by the Indian IT Act 2000 amendment 2008*, violation of which is an offence under national law.

2. The RCB campus network and Internet access resources are meant for official use and academic activities by faculty, staff and students of the Institute. Use of network resources for personal purposes is discouraged.

3. The network resources should be viewed with a sense of ownership and participation, and the users should actively help to prevent and to interdict any misuse. Procedures laid down, from time to time, regarding the management of network resources and computing facilities, must be understood and followed meticulously by the user community.

4. All information carried by the network is subject to scan 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 concordance with the Indian IT Act 2000.

5. The users are expected to be aware of the contents of this policy document, and agree to abide by its provisions. Once adopted, this policy will be publicly posted (for example, on the RCB web site), and all individuals who use RCB network resources will be made aware of this policy.

6. There will be a standing committee (comprising of PI/head of the division, Registrar, representative from Admin, System Administrator along with IT faculty in-charge that looks into all violations of this policy, and recommends suitable action.

Policy:

1. *Appropriate Use:*

1.1. The RCB 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 RCB community.

1.2. 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. It is the users' responsibility to protect their account from unauthorised use by changing the passwords periodically and using passwords that are not easily guessed.

1.3. Any attempt to circumvent system security, guess others' passwords, or in any way gain unauthorised access to local or network resources is forbidden. Users may not use another person's computing account, attempt to forge an account identity, or use a false account or email address.

1.4. Transferring copyrighted material to and from the RCB systems without express consent of the owner is a violation of international law. If done so, it will be the sole responsibility of the user.

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

1.6. The downloading of audio and video files is to be done strictly for official/academic purposes.

1.7. Recreational downloads and peer-to-peer connections for recreational purposes are banned.

1.8. Playing of games in RCB laboratories or using RCB facilities is strictly prohibited. Internet chat is also banned.

1.9. Access to sites that are banned under law or that are offensive or obscene is prohibited. This is also an offence under the Indian IT Act 2000.

1.10. 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 offence 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.

2. *Email Usage:*

2.1. The email service should be used primarily for official purposes.
2.2. To the extent possible, users are expected to use only their official email addresses provided by RCB for official communications.
2.3. Since email accumulates over time, the storage in email servers can overflow. Users must, therefore, regularly clean out their mail-boxes, failing which system managers may delete excess emails.
2.4. Use of the email service to send fraudulent, threatening, anonymous or harassing emails is prohibited.

3. *Use of only Licensed Software:*

3.1. Software programs are covered by copyrights and a licence is required for their use. Users must ensure that they have either a commercial or public licence (as in the case of 'free' software) for any software they install on the systems that they are responsible for.
3.2. Use and exchange of pirated software over the network is prohibited.
3.3. The downloading and use of software that is not characterized as public domain or 'free' is prohibited.

4. *System Protection:*

4.1. Users access the network via desktop/laptop machines on the campus network. Users are responsible and accountable for the usage of the systems allocated to them.
4.2. Users must take adequate measures to prevent network misuse from computer systems that they are responsible for.
4.3. Reasonable care should be taken to minimize the vulnerability of systems attached to the campus network. In particular, 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. User may ask IT division for any kind of support if needed.
4.4. 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. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems.

5. *Bring Your Own Device:*

5.1. At RCB we acknowledge the importance of mobile technologies in improving communication and productivity. In addition to the increased use of mobile devices, staff members/research personnel/students have requested the option of connecting their own mobile devices to RCB's network and equipment.

5.2. The personally owned mobile devices approved to be used at RCB are notebooks, smart phones, tablets, iPhone, removable media etc.

5.3. Employees when using personal devices for official/academic use will register the device with IT.

5.4. Personal mobile devices can only be used for the following purposes email access, internet access, telephone calls etc.

5.5. Each employee who utilises personal mobile devices agrees:

i. Not to download or transfer RCB or personal sensitive information to the device. Sensitive information includes intellectual property, other employee details etc.

ii. Not to use the registered mobile device as the sole repository for RCB's information. All RCB information stored on mobile devices should be backed up by the users.

iii. To make every reasonable effort to ensure that RCB's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected

iv. To maintain the device with current operating software, current security software, anti-virus etc.

v. Not to share the device with other individuals to protect the RCB data access through the device

vi. To abide by RCB's internet policy for appropriate use and access of internet sites etc. vii. To notify RCB immediately in the event of loss or theft of the registered device

vii. Not to connect USB memory sticks from an untrusted or unknown source to RCB's equipment.

5.6. All employees who have a registered personal mobile device for use acknowledge that the RCB:

i. Owns all intellectual property created on the device

ii. Can access all data held on the device, including personal data

iii. Users are responsible for back-up of data held on the device

iv. Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data

v. Has the right to deregister the device for RCB use at any time.

5.7. The following must be observed when handling mobile computing devices (such as notebooks, tablets and iPads):

i. Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
ii. Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
iii. Mobile devices should be carried as hand luggage when travelling by aircraft.

6. *Appropriate Use of Electronic Information Resources*

Electronic resources such as e-journals, e-books, databases, etc. made available by the RCB Library are for academic use. These resources can be searched, browsed, and material may be downloaded and printed as single copies of articles as is done in the case of printed library material. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited. Use of robots, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited. Any violation of this policy will result in penal action as per the rules and regulations of the Institute. I am aware that Systematic downloading will result in the publisher blocking the entire community of users at RCB from accessing these resources.

Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate. Depending upon the nature of the violation, the institute authorities may take an action by issuing a warning through disabling the account. In extreme cases, the account may be completely deleted and/ or the user prohibited access to IT facilities at RCB, and/ or sent to the Institute disciplinary action committee as constituted by the Institute authorities.

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.

7. *Installation Policy*

7.1. **Hardware**

Institute network user community needs to observe certain precautions while getting their computers or peripherals installed so that user faces minimum inconvenience due to interruption of services in case of hardware failures.

7.2. **Who is a Primary User?**

An individual in whose room the IT equipment is installed and is primarily used by him/her, is considered to be “primary” user. If an equipment has multiple users, none of whom are considered to be the "primary" user, So, the Head of the Lab / department is responsible for compliance.

7.3. **What are End User Computer Systems?**

Apart from the client PCs used by the users, the Institute will consider servers not directly under IT team administration, as end-user computers. If no primary user can be identified, the department Head/concerned PI/Authority must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers, which provide services to other users on the Intranet/Internet though registered with the RCB- IT, are still considered under this policy as "end-users" computers.

7.4. **Warranty & Annual Maintenance Contract**

Computers purchased by users under Core/Centre/Project should preferably be with 3-year to 5-year on-site comprehensive warranty. After the expiry of warranty, computers should be under the maintenance of RCB- IT. For extended the warranty of mission critical devices (like Firewall, Network Switches, Servers etc.) recommendations of IT Committee needs to be obtained.

7.5. **Power Connection to Computers and Peripherals**

All the computers and peripherals should be connected to the electrical point through UPS. Power supply to the UPS should never be switched off, as continuous power, supply to UPS is required for battery recharging.

7.6. **Network Cable Connection**

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

7.7. **Shifting Computer from One Location to another**

Computer system may be moved from one location to another by the concerned end-user with PI and subjected to the approval of Head Administration / Registrar and further intimated to RCB-IT/Store for record-keeping purposes.

7.8. **Operating System and its Updating**

Individual users should make sure that their respective computer systems have updated OS with the latest service packs and patches available on the internet. This is particularly important for all MS Windows / Other OS based computers (both PCs and Servers). Checking for updates and updating of the OS should be performed automatically and at least once in a month by the primary user/s, IT division may be requested for relevant support if needed.

7.9. **Antivirus Software and its updating**

Computer systems used in the RCB must have anti-virus software installed, and it should be active at all times. ***The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy***. It may be noted that for any antivirus software that is running on a computer, which is not updated or not renewed after its expiry period, user should inform IT section immediately.

7.10. **Remote Access & Monitoring**

Users are strictly restricted to share any remote access to outside user/agency, in case of any urgent need the user must inform IT division about their need and provide access under their supervision only. Also, the remote monitoring and maintenance of any Computer device shall be limited to authorized persons only.

7.11. **Backup of Data**

Individual users should perform regular backups of their important data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files impossible. IT division may be requested for relevant support if needed.

7.12. **Common Installation Clause for Hardware/Software**

7.12.1. All fresh/new/first installation of any hardware will be performed by agency if the installation scope/or charges are mentioned in the purchase order. Otherwise, the user should contact IT team for installation. If the installation can't be done by the IT team, then the standard procedure for maintenance may be followed.

7.12.2. Before initiate the purchase of any IT equipment (Laptop, Desktop, Workstation, Drive, Storage etc.) the PI/User shall vet the specification(s) with IT division / IT Committee (for big value and common uses item(s)) for their verification to avoid any mismatch in specification(s) at later stage. User should sign the invoice after installation of the hardware /Software product.

7.12.3. Installation will be performed and verified by the IT person. If the installation is not done in front of IT Person then user should inform IT team for post-verification.

7.12.4. All the hardware i.e. Laptop/Desktop should be password protected and the admin password should be shared with the PI/Reporting Authority.

7.12.5. Standard Password Policy

- Use minimum 12 characters
- Use a password combination of letters, numbers, special characters (upper and lower case)
- Same password may not be used for multiple logins

7.12.6. User should not save his/her personal data on official desktop/laptop.

7.12.7. The users are encouraged to turn- off their computers while not in use. This will ensure the safety of their devices from electric fluctuations and will save electricity. If the computer cannot be switched off, at least the screens may be switched off during non-active hours.

8. Disposal of IT Equipment's

Disposal of IT Device(s), RCB policy for disposal of goods, records, e-waste & item may be referred.

9. RCB Website

9.1. Advertisements, news and achievements on website at home page will be active for at least 7 days and will be replace as on when new information will be provided to IT team.

9.2. Each member of RCB is solely responsible for the content of web pages they create. The Concerned User/Division shall inform to IT at it@rcb.res.in in case of errors and omissions found/noticed in the RCB website. The email should be sent from a RCB email account.

9.3. Each faculty member & other officials at RCB is expected to contribute to and maintain an official web profile in a defined format. The minimum provided information on the web profile for faculty members should include:

- Research Profile
- Selected Publications
- Lab members etc.

9.4. It is the responsibility of PIs to keep their web profile up-to-date.

9.5. Requests for the creation of websites for individual centres of RCB should be sent to IT section. This will ensure that any new microsites added to the website conform to the technical and aesthetic norms of the RCB website. If required, user would be called for discussion with the IT Committee. A formal approval from Head Administration/ Registrar will be sought for each individual case.

9.6. Websites, either personally owned or run by respective centres may be hyperlinked to the RCB website. However, RCB IT team does not take responsibility for the content on such personal websites, nor does it monitor such content.

9.7. RCB does not tolerate discrimination or harassment of any person or community on the basis of religion, race, caste, gender and sexual orientation and web page content that violates this policy is strictly forbidden. Similarly, hate speech, inflammatory statements and offensive language are forbidden.

9.8. RCB prohibits posting of material under copyright without the permission of the owner, unless the license or copyright claim explicitly allows re-use or redistribution. (Assume that all material on the Web is copyrighted unless specified clearly)

9.9. Other than the above mentioned sections user may directly send a mail with the details of the program to administration and IT Section.

10. Development & Hosting of Web portals

The Concerned user(s) / division(s) shall take prior approval from the RCB IT Committee for any requirement of a web portal for their individual or division usage purpose. If not, RCB doesn't consider any authenticity to support and maintenance of that portal in future. In addition to this following guidelines shall be followed while developing a web portal:

1. Ensure that all websites hosted by the Ministries/Departments adhere to the Guidelines for Indian Government Websites (GIGW).
2. Develop a detailed schedule for conducting regular vulnerability assessments and penetration tests of all servers hosting web applications.
3. Perform comprehensive security audits of all applications whenever they are upgraded or customized.
4. Implement multi-factor authentication for all web applications to enhance the security of user accounts.
5. Establish a robust backup and disaster recovery strategy for web applications and associated data etc.

11. Internet Access Policy: For accessing RCB Internet, Captive Portal has been implemented

1. Functionality: For accessing RCB Internet, every individual will be facilitated with a login account i.e. Captive portal
2. Objective: To monitor any kind of suspicious activity into RCB network
3. Tracking Mode: Url based tracking, bandwidth tracking, usages tracking & threat tracking etc.
4. Proposed Policies under implementation of Captive Portal:
    - ✓ Default Firewall Security/Internet policies will be remained same
    - ✓ There will no data limit for RCB officials, however, session time out will be applicable for 8 Hour
    - ✓ User will be self-responsible for any kind of misuse of his/her credentials

Note: User manual of using Captive portal may be collected from IT division

11.1. **MAC binding:**

Alternatively, MAC binding may be implemented for each Research Personnel/ Student, administrative officers and staff. Their PC/Laptop/Mobile/Tablet's MAC ID will be registered with IT and allowed access to internet.

11.2. **Internet Access to the RCB Guest:**

RCB Guest will be allowed to limited access to RCB internet on their request, and will be facilitated with a temporary login account

Regional Centre for Biotechnology, Faridabad (RCB)
Undertaking with respect to RCB IT Usage Policy

To Whom this Document Concerns

All Users of IT infrastructure (Computers and the Network) at RCB.

Reason for Policy

This policy outlines the responsible use of the Information Technology Infrastructure at RCB.

Statement of Policy

All users of RCB internet and computing devices will be subject to the following **Acceptable Use Policy.**

1. **[Content]** I shall be responsible for all use of this network. In case I own a computer/computing device (notebooks, smart phones, tablets, iPhone, removable media) and decide to connect it to RCB network, I will be responsible for all the content on it, especially that which I make available to other users. In case I do not own a computer but am provided some IT resources by RCB, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on Computer Centre or Department machines).

2. **[Network]** I will be held responsible for all the network traffic generated by "my computer". I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipments, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Connecting of hubs, switches, repeaters, access points etc. to any of the network port of RCB is not permitted. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.

3. **[Academic Use]** I understand that the IT infrastructure at RCB is for academic/official use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law.

4. **[Identity]** I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use RCB IT resources to threaten, intimidate, or harass others.

5. **[Privacy]** I will not intrude on privacy of anyone. In particular I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

6. **[Monitoring]** I understand that the IT resources provided to me are subject to monitoring, with cause, as determined through consultation with the RCB management, 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. I authorize RCB to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of RCB network.

7. **[Viruses]** I shall maintain my computer on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, trojans, and other similar programs.

8. **[File Sharing]** I shall not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material). In particular, I have noted the following:

9. **[Security]** I understand that I will not take any steps that endanger the security of the RCB network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the RCB campus. In critical situations, RCB authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of RCB.

10. **[Penalties]** I understand that any use of IT infrastructure at RCB that constitutes a violation of RCB regulations or GOI regulation or is an offence under IT Act or other Acts framed by GOI from time to time, could result in administrative or disciplinary procedures apart from those admissible under relevant acts.

11. **[Indemnity]** I will not hold RCB responsible for loss of any data or financial losses due to activities conducted over the RCB network. Since research materials in RCB are accessible to others, I promise to not transmit data that does not belong to me using the RCB network, failing which I will be penalized appropriately. I understand that access to the RCB network will be terminated when I cease to be part of the academic programmes in RCB.

12. **[Indemnity]** I understand that RCB bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. I indemnify RCB against any and all damages, costs and expenses suffered by me arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by RCB.

I have read the statement of the IT usage policy and agree with the same.

Date: _____ Signature: _____

Place: _____ Name: _____

Designation: _____