SHRI GURU RAM RAI
UNIVERSITY
Quest for Excellence

I T Policy

I T- POLICY & GUIDELINES

SGRR University
Patel Nagar
Dehradun

May 16, 2022

SHRI GURU RAM RAI UNIVERSITY
Registrar
DEHRADUN

SHRI GURU RAM RAI UNIVERSITY
Registrar
DEHRADUN

1. Abbreviation

Sl. No.	Abbreviation	Description
1.	SGRRU	SGRR University
2.	CA	Competent Authority
3.	IA	Implementing Agency
4.	LAN	Local Area Network
5.	GoI	Government of India
6.	IT	Information Technology
7.	ICT	Information and Communication Technology
8.	IP	Internet Protocol
9.	DHCP	Dynamic Host Configuration Protocol
10.	IR	Institutional Repository
11.	EULA	End User License Agreement
12.	CAPEX	Capital Expenditure
13.	OPEX	Operational Expenditure

2. Introduction

SGRR University (SGRRU) provides IT resources to support the educational, instructional, research, and administrative activities of the University and to enhance the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work. These resources help them to remain well informed and carry out their functions in an efficient and effective manner.

This document establishes specific requirements for the use of all IT resources at SGRRU. This policy applies to all users of computing resources owned or managed by SGRRU. Individuals covered by the policy include (but are not limited to) SGRRU faculty and visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, affiliated colleges and any other entity which falls under the management of SGRR University accessing network services via SGRRU's computing facilities.

For the purpose of this policy, the term 'IT Resources' includes all university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Misuse of these resources can result in unwanted risks and liabilities for the university. It is, therefore, expected that these resources are used primarily for university-related purposes and in a lawful and ethical way.

3. Scope

This policy governs the usage of IT Resources from an end user's perspective. This policy is applicable to all individuals/ users/ entities, as defined in Section 2, who use the IT Resources of SGRRU.

4. Objective

The objective of this policy is to ensure proper access to and usage of SGRRU's IT resources and prevent their misuse by the users. Use of resources provided by SGRRU implies the user's agreement to be governed by this policy.

- University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

5. Roles and Responsibilities

The following roles and responsibilities are envisaged from each entity respectively.

1) SGRRU shall implement appropriate controls to ensure compliance with this policy by its users. Computer Centre shall be the primary Implementing Agency and shall provide necessary support in this regard.
2) Computer Centre shall ensure the resolution of all incidents related to the security aspects of this policy by their users. Implementing Agency shall provide the requisite support in this regard.
3) Use SGRRU's IT resources for those activities that are consistent with the academic, research and public service mission of the University and are not "Prohibited Activities".
4) All users shall comply with existing national, state and other applicable laws.
5) Abide by existing telecommunications and networking laws and regulations.
6) Follow copyright laws regarding protected commercial software or intellectual property.
7) As a member of the University community, SGRRU provides the use of scholarly and/or work-related tools, including access to the Library, certain computer systems, servers, software and databases and the Internet. It is expected from University Community to have a reasonable expectation of unobstructed use of these tools, certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources. Authorized users can expect their right to access information and to express their opinion to be protected as it is for paper and other forms of no electronic communication.
8) Users of SGRRU shall not install any network/security device on the network without consultation with the IA.
9) It is the responsibility of the University Community to know the regulations and policies of the University that apply to the appropriate use of the University's technologies and resources. University Community is responsible for exercising good judgment in the use of the University's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.
10) As a representative of the SGRRU community, each individual is expected to respect and uphold the University's good name and reputation in any activities related to the use of ICT communications within and outside the university.
11) Competent Authority of SGRRU should ensure proper dissemination of this policy.

6. Acceptable Use

- An authorized user may use only the IT resources he/she has authorization. No user should use another individual's account, or attempt to capture or guess other users' passwords.
- A user is individually responsible for the appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware. Therefore, he/she is accountable to the University for all use of such resources. As an authorized SGRRU user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of SGRRU or a personal computer that is connected to the SGRRU campus-wide Local Area Network (LAN).
- The university is bound by its End User License Agreement (EULA), respecting certain third party resources; a user is expected to comply with all such agreements when using such resources.
- Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access.
- No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- Users must comply with the policies and guidelines for any specific set of resources to which he/she have been granted access.
- When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

7. Privacy and Personal Rights

1) All users of the university's IT resources are expected to respect the privacy and personal rights of others.
2) Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).
3) While the University does not generally monitor or limit the content of information transmitted on the campus-wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.

8. Privacy in Email

While every effort is made to ensure the privacy of SGRRU email users, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct University business, there may be instances when the University, based on approval from the competent authority, reserves and retains the right to access and inspect stored information with the consent of the user.

9. User Compliance

When an individual uses SGRRU's IT resources and accepts any University issued computing accounts, it means that the individual agrees to comply with this and all other computing-related policies. It is the responsibility of the individual to keep oneself up-to-date on changes in the IT policy of SGRRU and adapt to those changes as necessary from time to time.

10. Access to the Network

10.1. Access to Internet and Intranet

1) A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the University Campus-wide LAN.
2) SGRRU shall maintain two independent networks, i.e. Internet and Intranet. Both the networks shall not have any physical connection/devices between them. Endpoint compliance shall be implemented on both networks to prevent unauthorized access to data.
3) Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

10.2. Access to SGRRU's Wireless Networks

For connecting to SGRRU's wireless network, the user shall ensure the following:

1) A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the SGRRU's wireless network.
2) Wireless client systems and wireless devices shall not be allowed to connect to the SGRRU's wireless access points without due authentication.
3) To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

GURU RAM RAI UNIVE

10.3. Filtering and blocking of sites:

1) Computer Centre or any other Implementing Agency (IA) may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.
2) Computer Centre or any other Implementing Agency (IA) may also block content that, in the opinion of the university, is inappropriate or may adversely affect the productivity of the users.

11. Monitoring and Privacy

1) Computer Centre or any other Implementing Agency (IA) shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.
2) IA/Nodal Agency, for security-related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on University provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.
3) IA may monitor users' online activities on the University network, subject to such Standard Operating Procedures of GoI norms.

12. E-mail Access from the University Network

1) E-mail service authorized by SGRRU and implemented by the Computer Centre shall only be used for all official correspondence.
2) More details in this regard are provided in the "E-mail Usage Policy of SGRRU".

13. Access to Social Media Sites from SGRRU Network

1) Use of social networking sites by SGRRU users is governed by the "Framework and Guidelines for Use of Social Media for Government Organizations".
2) User shall comply with all the applicable provisions under the IT Act 2000 while posting any information on social networking sites.
3) User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.
4) User shall report any suspicious incident as soon as possible to the competent authority.
5) User shall always use high-security settings on social networking sites.

RAM RAI UNI

6) User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
7) Users shall not disclose or use any confidential information obtained in their capacity as an employee of the university.
8) User shall not make any comment or post any material that might otherwise cause damage to SGRRU's reputation.

14. Use of IT Devices Issued by SGRRU

IT devices issued by the SGRRU to a user shall be primarily used for academic, research and any other university-related purposes in a lawful and ethical way and shall be governed by the practices defined in the Section "Use of IT Devices on SGRRU Network". The aforesaid section covers best practices related to the use of desktop devices, portable devices, external storage media and peripherals devices such as printers and scanners.

15. Security Incident Management Process

1) A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of the University's data.
2) IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of the university.
3) Any security incident noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA.
4) Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the IA shall be done as per the IT Act 2000 and other applicable laws.
5) IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny or release of logs.

16. Intellectual Property

Material accessible through the SGRRU's network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, and trademarks, trade secrets or other proprietary information. Users shall not use SGRRU's network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

17. Enforcement

1) This policy is applicable to all the users of SGRRU as specified in Section 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.
2) Each entity of SGRRU shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the user entities in this regard.

18. Deactivation

1) In case of any threat to the security of SGRRU's systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the IA.
2) Subsequent to such deactivation, the concerned user and the competent authority of the university shall be informed.

19. Audit of SGRRU Network Infrastructure

The security audit of NIC network infrastructure shall be conducted periodically by an organization approved by the university.

20. Review

Future changes in this Policy, as deemed necessary, shall be made by the Technical Committee (ICT) with the approval of the Competent Authority of the university.

21. IT Hardware Installation Policy

The University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

21.1. Who is the Primary User

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be the "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the Department Head should make an arrangement and make a person responsible for compliance.

21.2. What are End User Computer Systems?

Apart from the client PCs used by the users, the university will consider servers not directly administered by Computer Centre, as end-user computers. If no primary user can be identified, the department 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 Computer Centre, are still considered under this policy as "end-users" computers.

21.3. Warranty & Annual Maintenance Contract

Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite comprehensive warranty. After the expiry of the warranty, computers should be under an annual maintenance contract. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer Centre from time to time.

21.4. Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. The power supply to the UPS should never be switched off, as a continuous power supply to UPS is required for battery recharging, till such instances wherein the UPS is to be left unattended. Further, these UPS systems should be connected to the electrical points that are provided with the proper earthling and have properly laid electrical wiring.

21.5. Network 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.

21.6. File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through the network, they should be protected with passwords and also with read-only access rule.

21.7. Maintenance of Computer Systems provided by the University

For all the computers that were purchased by the university centrally and distributed by the Estate Branch, the University Computer Maintenance Cell attached to the Computer Centre will attend to the complaints related to any maintenance related problems.

GURU RAM RAI UNIVERSITY DEHRADUN

22. Software Installation and Licensing Policy

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, the University IT policy does not allow any pirated/unauthorized software installation on the university-owned computers and the computers connected to the university campus network. In case of any such instances, the university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

22.1. Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through the internet. Checking for updates and updating the OS should be performed at least once a week or so.

University as a policy encourages the user community to go for open-source software such as Linux, and Open office to be used on their systems wherever possible.

22.2. Use of software on Desktop systems

a. Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.

b. Any software installed should be for activities of the university only.

22.3. Antivirus Software and its updating.

Computer systems used in the university should 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.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

22.4. Backups of Data

Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc.

23. Use of IT Devices on SGRRU Network

This section provides the best practices related to the use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners on SGRRU's network.

23.1. Desktop Devices

1) Use and Ownership

Desktops shall normally be used only for transacting the university's works. Users shall exercise their own good judgment and discretion towards the use of desktop devices for personal use to the minimum extent possible.

2) Security and Proprietary Information

a. User shall take prior approval from the IA to connect any access device to the SGRRU's network.

b. User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords as per the password policy of the application.

c. All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.

d. Users shall ensure that updated virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.

e. The user shall report any loss of data or accessories to the IA and competent authority of SGRRU.

f. User shall obtain authorization from the competent authority before taking any SGRRU issued desktop outside the premises of the university.

g. Users shall properly shut down the systems before leaving the office/ department.

h. Users shall abide by instructions or procedures as directed by the Computer Centre from time to time.

i. If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to the IA (Computer Centre) for corrective action.

RI GURU RAM RAI UNIVERSITY DEHRADUN

23.2. Sharing of data

Users shall not share their account(s), passwords, Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

23.3. Use of Portable devices

Devices covered under this section includes SGRRU issued laptops, mobiles, iPads, tablets, PDAs etc. Use of the devices shall be governed by the following:

a. User shall be held responsible for any unauthorized usage of their SGRRU issued access device by a third party.
b. Users shall keep the SGRRU issued devices with them at all times or store them in a secured location when not in use. Users should not leave the devices unattended in public locations (e.g. classrooms, meeting rooms, restaurants etc.).
c. Users shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong as the device may support and should be as per the password policy of the application.
d. Computer Centre shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls shall be enabled, if possible.
e. Users shall wipe or securely delete data from the device before returning/ disposing of it.
f. Lost, stolen, or misplaced devices shall be immediately reported to the IA/ and the competent authority.
g. When installing software, the user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

24. Network (Intranet & Internet) Use Policy

Network connectivity provided through the University referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy. The Computer Centre is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to Computer Centre.

24.1 IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the Computer Centre. Following a systematic approach, the range of

IP addresses that will be allocated will be based on Virtual LAN (VLAN) created against each entity or objective. Any device connected to the network will be allocated IP address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.
As and when a new computer is installed in any location, it will be allocated as per the DHCP pool policies.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. The IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

24.2. DHCP and Proxy Configuration by Individual Departments /Sections/ Users

Use of any computer at the end-user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered an absolute violation of IP address allocation policy of the university. Similarly, the configuration of proxy servers should also be avoided, as it may interfere with the services run by the Computer Centre.

Even the configuration of any computer with an additional network interface card and connecting another computer to it is considered a proxy/DHCP configuration.

Non-compliance with the IP address allocation policy will result in disconnecting the port from which such a computer is connected to the network. The connection will be restored after receiving written assurance of compliance from the concerned department/user.

24.3. Running Network Services on the Servers

a. Individual departments/individuals connecting to the university network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the Computer Centre in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy and will result in the termination of their connection to the Network.

b. Computer Centre takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.

c. Computer Centre will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

d. Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes.

e. Network traffic will be monitored for security and for performance reasons at the Computer Centre.

f. Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

24.4. Internet Bandwidth obtained by Other Departments

a. Internet bandwidth acquired by any department of the university under any research programme/project should ideally be pooled with the university's Internet bandwidth, and be treated as the university's common resource.

b. Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such a network should be totally separated from the university's campus network. All the computer systems using that network should have separate VLANs based on grouping criteria.

c. IP address scheme (private as well as public) and the university gateway should not be specified as an alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the university IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to Computer Centre.

d. Non-compliance with this policy will be a direct violation of the university's IT security policy.

25. Email Account Usage Policy

SGRRU provides official email access privileges to its users. In an effort to handle the efficient information dissemination among the administration, faculty members, staff and students, it is recommended to avail official email with SGRR University's domain.

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to http://gmail.com with their User ID and password. For obtaining the university's email account, the user may contact Computer Centre for the email account and default password by submitting an application in a prescribed proforma.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1) The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2) Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3) While sending large attachments to others, the user should make sure that the recipient has an email facility that allows him to receive such large attachments.
4) User should keep the mailbox used space within about 80% usage threshold, as a 'mailbox full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5) User should not open any mail or attachment that is from an unknown and suspicious source. Even if it is from a known source, and if it contains any attachment that is of suspicious in nature or looks dubious, the user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have the potential to damage the valuable information on your computer.
6) User should not share his/her email account's credentials with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
7) Users should refrain from intercepting, or trying to break into others' email accounts, as it is infringing the privacy of other users.
8) While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
9) Impersonating the email accounts of others will be taken as a serious offence under the IT security policy.
10) It is ultimately each individual's responsibility to keep their e-mail account free from violations of the university's email usage policy.
11) All the emails detected as spam mails go into the SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any

important mail wrongly stamped as SPAM mail and went into this folder. It is recommended to empty this folder as frequently as possible.

The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other service providers such as Gmail, Hotmail, Yahoo, Rediff Mail etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

26. Institutional Repository (IR)

SGRR University shall be providing services related to Institutional Repository (IR) through the Central Library of the university as per the following policies

26.1. What is IR (Institutional Repository)?

A University-based institutional repository (IR) is a set of services that a University Library offers to the members of its community for the management and dissemination of digital materials created by the University or institution and its community members. It is most essentially an organizational commitment to the stewardship of these digital materials including long-term preservation, access and dissemination of e-resources of an organization to its users.

26.2. What Does IR contain?

IR of the institution contains a wide variety of documents depending on the policy of the institution. Most common are the outputs of research journal articles (pre-print and post-print), conference papers, technical reports, computer programs, preservations, technical manuals, video and audio recordings, e-Books, Seminar and Webinar lectures, Theses and Dissertations Rare books etc. Grey literature is as important as published outputs in the IR. Institutional Repository (IR) also contains other items such as convocation addresses, student handbooks, as well as teaching materials quote sources which suggest that a repository should be integrated with the University's course management system and display e-learning features. In practice, however, the SGRR University institution repository (IR) will provide a basic repository of such resources available online which focuses on research and academic publications.

26.3. Who will be entitled to access SGRR University IR?

Mainly the bonafide members i.e. faculty members, research scholars, students and other staff members having institutional e-mail IDs (i.e. @sgrru.ac.in) are authorised members to access the IR of SGRR University.

26.4. How will you access the IR?

The registered members through their institutional e-mail address can log in to IR link http://SGRRUir.inflibnet.ac.in and browse the SGRRU IR and can download digital materials in pdf format purely for their academic purpose subject to the provision of giving general information of the member provided in the SGRR University IR portal.

26.5. Validity Period of Accessibility of IR

Teachers, researchers and students are authorized to access SGRRU IR as long as they are in the University. The moment the tenure in the University or the course is completed and the no dues certificates are issued from the University Library authority, the validity of access to SGRRU IR will be withdrawn.

26.6.Copyright Violation on IR Use

SGRR University IR digital materials are mainly grey literature. Any downloaded digital materials from the IR come under the purview of copyright. The downloaded permissible materials cannot be reprinted and sold in the market for commercial purposes further. If any member found violating such copyright act shall be treated as per the provisions of copyright act-1957. The created user-id and password are person-specific and cannot be transferred to any other person and are subject to the violation of SOPs of SGRR University IR.

27. Disposal of ICT equipment

The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the university.

28. Budgetary provisions for ICT

At SGRR University, the use of ICT facilities have been encouraged as it is located in a remote area of the country. This has always been leverage to march shoulder to shoulder with the rest of the universities. In view of these scenarios, SGRRU intends to provide budgetary provisions as follows:

SHRI GURU RAM RAI UNIVERSITY Registrar DEHRADUN

1) Budgetary provisions should be made under recurring grants (OPEX) to maintain all the existing ICT infrastructure for the smooth functioning of all the ICT enabled services.
2) Adequate budgetary provisions under capital head (CAPEX) should be kept for upgradation and augmentation of ICT infrastructure
3) Budgetary provisions under capital grants should also be allocated for the implementation of newer ICT solutions from time to time.
4) In SGRRU, there has been a substantial increase of enrolment of students every year. Keeping in view of this increase and for the benefit of the students, proper allocation of a budget of the university should be earmarked for ICT facility, particularly for students.

29. Breach of This Policy

Users is encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Helpdesk admin@sgrru.ac.in. On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user's access to University's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

30. Revisions to Policy

The University reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy, which is available on the SGRRU website and continuing to use the University's IT Resources following any update it is considered accepted on the revised terms of this Policy.

31. Contact Us

If you have any queries in relation to this policy, please contact:

IT Head

Phone:

Email:

SHRI GURU RAM RAI UNIVERSITY
Registrar
DEHR

Appendix – I: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID

(For Teachers & Staff only)

First Name	:
Middle Name	:
Last Name	:
Department/ Branch	:
Current Email address*	:
Mobile Number	:

Note:

1. Please spell the names and all other information sought above correctly.
2. This Email address should be currently used by you.
3. The filled-in form should be submitted after getting duly signed by the respective Head of the Department/ Controlling Officer.
4. An official Email address would be created within 48 hrs. - 72 hrs.
5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department/ Controlling Officer)

Appendix – II: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID

(For Research Scholars only)

First Name	:
Middle Name	:
Last Name	:
Department	:
Name of the PI	:
Name of the Project	:
Duration of Research	:
Current Email address*	:
Phone Number	:
Admission Year*	:

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled-in form should be submitted after getting duly signed by the respective Head of the Department and Principal Investigator.
4. An official Email address would be created within 48 hrs. - 72 hrs.
5. Information regarding the official Email address created would be sent to your current Email address.

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Head of the Department)

GRANT AN OFFICIAL E-MAIL ID PLEASE.

(Signature of the Principal Investigator)

Appendix – III: Wi-Fi Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS

(For Students only)

Name	:	
Father's Name	:	
Gender	:	
DoB	:	
Department	:	
Course	:	
Semester	:	
Roll No.	:	
Email address*	:	
Mobile Number	:	

SHRI GURU RAM RAI UNIVERSITY
Registrar
DEHRADUN

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled-in form should be submitted after getting duly signed by the respective Head of the Department.

(Signature of the Head of the Department)

Appendix – IV: Wi-Fi Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS

(For Employees only)

Name	:	
Father's Name	:	
Gender	:	
DoB	:	
Department/ Branch	:	
Email address*	:	
Mobile Number	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled-in form should be submitted after getting duly signed by the respective Controlling Officer.

(Signature of the Controlling Officer)

Addendum

IT. Policies 16/5/2022

Data Center Management Policy-

Datacenter policy is applicable to ensure the basic principles and procedures for smooth operations/upgrades, availability of systems and applications, data and information security and reliability.

Scope

This policy applies to all Datacenters / Server rooms/ Network rooms / Utility rooms/Communication rooms used for performing any type of computer technology work within the premises (private cloud), hosted outside

People Role mapping to Datacenter Operations

The following people roles are mapped to Datacenter Operations:

Data Center Employee: A small team of IT employees who work at the Data Center. These will mainly be of the Group Infrastructure/Local IT team respectively.

Authorized Staff: Employees who are authorized to gain access to the Data Center but who do not work for the Data Center. These will be utility service providers like the Security team, estate team, admin team etc.

Authorized Vendor: All contractors/service providers who, through contractual arrangement and appropriate approvals, have access to the Data Center.

Visitors: All other employees who may occasionally visit the Data Center but are not authorized to be in the Data Center without an escort.

Hosting Datacenter Staff: This will be for staff of the hosting service provider, whose Datacenter is/may be used for hosting servers and IT pieces of equipment.

Equipment's in Datacenter

There are 2 parts which get covered in this section.

First is which equipment's will get hosted in the Datacenter. The List of equipment's which will get hosted in the Datacenter is as follows –

Servers. Storages & Racks.

Network Equipment's & Appliances.

Security Equipment & Appliances.

Associated IT Peripherals.

Central Communication equipment (Audio / Video/ Voice / Data) Cooling equipment Safety equipment. Any other critical IT equipment based on approval from Group IT Infrastructure Head.

Capacity Management

Capacity demands shall be monitored and projections of future capacity requirements will be made to ensure that adequate processing power and storage are available. These projections take into account new business and system requirements and current and projected trends in the Resource Centre's information processing.

The projections identify trends in usage, particularly in relation to business applications or management information system tools.

The IT team will monitor the following parameters for Capacity Calculation:

1. Technology Hardware – Server Usage, Network bandwidth (LAN, Wi-Fi, MPLS) usage, Storage Usage trend, Firewall Usage. Software – Licenses (OS, Application, AV)
2. Infrastructure Physical – UPS, AC, Battery Bank, Fireproof cabinet, Fire Fighting equipment, Server Rack, Lighting, CCTV Service – AMC with vendors Communication – Telephone, Internet, VPN, Mailing Spares Any Addition / Up-gradation will be approved by Infrastructure head after SCR filling. Network & Communication Network cable laying should be done from below the raised flooring. Monitoring devices to be installed to provide alerts in case of any abnormalities (fire, smoke, power outage etc.).
3. Placing Equipment's in the Datacenter
4. Datacenter Access Authorization
5. Datacenter Maintenance
6. Datacenter Hygiene

Network Management Policy

The organization will adopt a uniform set of standards, installation practices, processes, procedures, and operational criteria in the construction, use, and ongoing management of the Institution, and network to ensure its security, safety, efficient use and seamless availability across the group.

The infrastructure team will manage and administer the inter-unit connectivity with the help of the IT team. Physical/wired connectivity within the institution will be established as per the requirement shared by the institution/office layout. Wireless connectivity will be established in the staff sitting/movement area

Network Security—

Cloud Usage Policy-

Overview & Purpose-

1. This Policy defines the Process to follow while deciding on application and data hosting on cloud servers and practices to follow in order to protect internal, confidential and sensitive information being stored, processed or transmitted by cloud computing services.
2. **Scope**

   This policy applies to all Existing and new Cloud services in Group.
3. **Policy**

   This policy is a statement of the Organization's commitment to ensuring that all its legal and policy compliance requirements are met in the usage of cloud services.

Authorizing Cloud Hosting-

Business Need Justification.

- Alternates if any.
- Data Security.
- Exit & Termination Clauses.
- Compliance Adherence.
- Policy Adherence.
- Bandwidth & Connectivity.
- User Awareness.
- Support and Maintenance

Legalities-

Termination of Cloud Services
Cloud Access Permission

IT Service Management Policy-

The purpose of this policy is to ensure that unexpected disruptive events are managed and responded to with the objective of controlling the impact of the group's working

The aim of this document is to define the direction, principles and basic rules of IT Service Management to ensure high customer satisfaction.

Policy-

This policy is intended to provide a high quality of services to IT, users, by defining SLAs and best practices and Monitoring IT assets. The group IT team is responsible for all the activities involved in designing, creating, delivering, supporting and managing the lifecycle of IT services.

IT Services-

There are various forms of IT Services that the SGRR IT Team provides. Some of the key ones (refer service Catalogue for a complete list) are as below-

ERP E-Mail.

IT Assets (PC, Laptop, Printers, UPS etc.) installation & maintenance CCTV setup and maintenance. Internet Services Collaboration services (Video Conferencing etc.)

Network Connectivity Patch Management.

Anti-virus management. ETC.

Software Development Lifecycle Policy-

This policy applies to all types of software development

Backup Management Policy

The backup Management policy is a key part of Business Continuity & IT Service Management. A backup will ensure the availability of data in case of a disaster or an event.

The purpose of this policy is to ensure that the critical information assets are always backed up, and are also recoverable as and when required. This will also ensure that all backups of information assets are in accordance with the approved business and technical requirements.

- Planned & Unplanned Backups-
- A backup Plan Sheet is a planned way of doing a backup. However, that doesn't mean that unplanned backups can't be taken.

- The Backup Plan sheet will generally include -
- Information to be backed up;
  a)-The system where this information is currently stored (system name)
  b) - Type of Asset (physical/virtual); o Folders / Databases;
- Type of Backup (online/offline and /full);
- Backup periodicity (daily/weekly/monthly);
- Retention period of the backup;
- Storage facility;
- IT Admin & Business user details.

Backup planning format, to be controlled by Group Infrastructure team
The unplanned backups can be conducted by the related IT teams and records to be maintained.

Backups & Media -The sole discretion of appropriate Backup Media lies with the Location IT teams and the IT Infrastructure team. However they need to make a Backup Media Plan form, and take due approvals from the Group Compliance Officer.

Storage of Backups.

Asset Management Policy
The Asset Management policy encompasses planning, demand, acquisitions, usage, maintenance, and disposal of information assets in order to achieve efficient and effective service delivery.

Policy –
Information Assets –
The policy of Asset Management is applicable to the below specific information assets.
These are (including but not limited to)
Hardware Assets for Data Processing: Servers, Storages, Other Data Processing Hardware.

Hardware Assets for Networking & Security:
Switches, Routers, Firewalls, Load Balancers, Appliance based solutions, and other Network & Security Appliances.

Software Assets:

- Perpetual or subscription-based.
- Backup Infrastructure: Servers, Storages, Cloud.
- Consumables: Hard Disks, RAM, Pen Drives, Others.
- Asset Management Attributes Asset Management is divided into different attributes, which are Asset Ownership; Control; Custodianship & Usage Rights

Quest for Excellence”

SHRI GURU RAM RAI UNIVERSITY

(Established By Govt. of Uttarakhand, vide Shri Guru Ram Rai University, Act no. 3 of 2017)