स्वामी राम हिमालयन विश्वविद्यालय
Swami Rama Himalayan University

COMPUTER AND NETWORK USAGE POLICY

Approved by the Board of Management in its 1st Meeting held on
18th November, 2013

Swami Rama Himalayan University

Swami Ram Nagar, Jolly Grant- 248 016, Dehradun, Uttarakhand

SWAMI RAMA HIMALAYAN UNIVERSITY

Computer and Network Usage Policy (IT Policy)

Computing Resources

As part of its educational mission, the Swami Rama Himalayan University acquires, develops, and maintains computers, computer systems and networks. These computing resources are intended for University-related / Educational purposes, including direct and indirect support of the University's instruction, research and service missions; University administrative functions; student and campus life activities; and for free exchange of ideas within the University community and wider local, national, and world communities.

Applicability

i. This policy applies to all users of University computing resources, whether affiliated with the University, and for use of those resources, whether on campus or other remote locations.

ii. "Users" are defined as anyone who uses University systems or networks including employees, students, parents, vendors, contractors, support personnel etc.

General Guidelines

Users of University computing resources shall comply with applicable national laws, applicable State Laws, University rules and policies, and the terms of applicable contracts including software licenses while using University computing resources. Examples of applicable laws, rules and policies include the laws of privacy, copyright, trademark, obscenity and child pornography; the IT Act 2000, which prohibits "hacking," "cracking" and similar activities.

Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks.

Users should not state or imply that they speak on behalf of the University or use University trademarks and logos without authorization to do so. Authorization to use University trademarks and logos on University computing resources may be granted only by the Vice Chancellor. The use of appropriate disclaimers is encouraged.

Rights & Responsibilities

1. Faculty, staff, and students with authorized accounts may use the computing and IT facilities for academic purposes, official University business, and for personal purposes so long as such use:

Registrar
Swami Rama Himalayan University

i. Does not violate any law, University policy or IT act of the Government of India.

ii. Does not interfere with the performance of Swami Rama Himalayan University and duties or work of an academic nature.

iii. Does not result in commercial gain or private profit other than that allowed by the Swami Rama Himalayan University.

Account Security & Privacy

1. 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 unauthorized use by changing passwords periodically and using passwords that are not easily guessed. Sharing of passwords for any purpose whatsoever is strictly prohibited. Users may share the required files through sharing software with proper ACL (Access Control list).

2. Any attempt to circumvent system security, guess others' passwords, or in any way gain unauthorized 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 e-mail address.

3. Transferring copyrighted materials to or from the Swami Rama Himalayan University systems without express consent of the owner is a violation of international law.

Password Policy

Passwords are a critical aspect of computer security forming the front line of protection for user accounts. A poorly chosen password can result in the compromise of the entire University's network. As such, all University students and users (including contractors and vendors with access to University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

1. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a semi-annual basis.

2. All production system-level passwords must be part of the IT Services administered global password management database.

3. All user-level passwords (e.g., email, web, desktop computer, etc.) must have

Registrar
Swami Rama Himalayan University

a. Maximum password age of 180 days

b. Minimum password age of 2 days

c. Exhibit complexity by

   i. Not containing all or part of the user's account name

   ii. Contain characters from three of the following four categories:

      1. Uppercase characters (A through Z)

      2. Lowercase characters (a through z)

      3. Base 10 digits (0 through 9)

      4. Non-alphabetic characters (for example, !, $, #, %)

d. Maintain a password history of 2 passwords and not allow reuse

e. Must be a minimum of 8 characters

Commercial Use Policy

i. Computing resources are not to be used for personal commercial purposes or for personal financial or other gain.

ii. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of University equipment.

iii. In addition, use of the internet for commercial gain or profit is not allowed. If done so, it will be sole responsibility of the user.

E-Mail policy

All communication though E-mail can be authenticated if sent through srhu.edu.in , implying that all other mails sent through other domains may not be considered official and no action can be taken on that.

1. To the extent possible, users are expected to use only their official email addresses provided by Swami Rama Himalayan University for official communications with other members of the University.

2. It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. Neither is any form of commercial advertising, or soliciting allowed. Spamming is strictly disallowed. Subscribing to mailing lists outside the Institute is an individual's responsibility.

Registrar
Swami Rama Himalayan University

3. Shared email accounts for any purpose whatsoever are not allowed. Any special accounts, if need to be set up for conferences and other valid reasons as determined by the university authorities, must have a single designated user.

4. An employee who leave the University after retirement/re-employment or otherwise can have his E-mail account validated up to the Notice period specified in his/her appointment terms. Account will be disabled / deactivated from the date of relieving.
5. Any e-mail account which remains unused for more than six months should automatically be removed.

Forwarding of E-mail

Users who choose to have their email forwarded to an unofficial e-mail address will do so at their own risk. Swami Rama Himalayan University is not responsible for any e-mail beyond delivery to Swami Rama Himalayan University official accounts. Users are however responsible for official e-mail as outlined above.

Wireless Policy

For the purposes of this document, we refer only to wireless transmission using radio frequency (RF). As wireless is a shared media and easily intercepted by a third party, wireless users are encouraged to use some type of encryption. Use of the WPA2-AES, WPA2-TKIP or WPA2-ENTERPRISE encryption protocols is suggested to encrypt wireless communication.

i. Improperly configured wireless access points (WAPs) might cause denial of service to legitimate wireless users and can also be used to subvert security. Wireless access points must be authorized by the Systems Administrator

ii. Recreational downloads and peer to peer connections for recreational purposes are not allowed unless it is academic requirement.

iii. To the extent possible, users are expected to connect only to the official Swami Rama Himalayan University WiFi network for wireless access. Setting up of unsecured Wi-Fi systems on the Swami Rama Himalayan University network is prohibited in accordance with Government of India guidelines.

iv. Users are expected to take proper care of network equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility.

Virtual Private Network (VPN) Policy

i. A VPN provides secure encrypted access between a client and the VPN server. They are most commonly used to secure access to a trusted network from remote, untrusted networks.

ii. VPN servers must be authorized by the in-charge of the facility.

Registrar
Swami Rama Himalayan Univer

Lab Use Policy

Swami Rama Himalayan University provide all faculty, students and staff with a modern, fully networked computing Labs and IT environment for academic use only . Users of Swami Rama Himalayan University computing, networking and IT facilities are expected to abide by the following rules, which are intended to preserve the utility and flexibility of the system, protect the privacy and work of students and faculty, and preserve our right to access the international networks to which the system is connected. In case of complaints, appropriate action to be taken will be decided and taken by the Swami Rama Himalayan University Authorities.

1. Downloading and installing of new software has to be done with the explicit consent of the respective in-charges. Installation of unlicensed software on Swami Rama Himalayan University facilities, or on individual machines connected to the SRHU network, is strictly prohibited.

2. Only Approved Software is allowed to be installed in University Computing labs.

3. Software necessary to implement practical requirements of University Syllabus for various courses are allowed in Labs. Concerned head of Deptt. Or Syllabus Coordinator is responsible to submit Software requirements according to Syllabus and IT Center will maintain availability of those software' in Computing labs.

4. Playing of Games in University laboratories or using University facilities for same is strictly prohibited

5. Display and storage of offensive material like storing pornographic material on the disk, viewing pornographic material on the terminals is strictly disallowed and serious action will be taken against offenders.

6. Wasting of resources like unnecessary downloads from Internet , giving accounts to other persons, sometimes outsiders, , using personal account to do outside work for which the individual is paid are not allowed.

Supported Software

Unless otherwise specified, the following is a list of software approved by the University and supported by IT Center. These applications will be installed and maintained for all security patches and updates on computers owned by the University:

a. Base Operating System (Microsoft Windows, Linux, Mac OSX)

b. Office Automation Suite (Microsoft Office)

c. Acrobat Reader and generator (if required)

Registrar
Swami Rama Himalayan University

d. File compression utility

e. Email client

f. Web Browser (Microsoft Internet Explorer / Mozilla Firefox or Google Chrome)

g. Anti Virus software (Security essentials, Windows defender etc.)

h. ORACLE client (if required)

i. Licensed Domain specific software on lab computers

j. Educational Software and software Under MSDN subscription on Lab Computers

k. E-book readers (Microsoft, Kindle or other standards compliant reader)

Web Pages Policy

i. Official University pages (including colleges, departments, bureaus, centers, institutes, etc.) represent the University and are intended for the official business functions of the University.

ii. Each official home page must use an address that ends with www.srhu.edu.in and be registered with the University's Web administrator who will then include it as a link in the Swami Rama Himalayan University Website or intranet.

iii. User pages represent the individual in his or her primary role as a Swami Rama Himalayan University user. Incidental personal information on user pages is deemed acceptable so long as it does not interfere with the function or desired presentation of the unit, cause disruption of normal service, incur significant cost to the University or result in excessive use of resources.

iv. Faculty and staff who wish to publish substantial personal information not related to their University functions should use an Internet service provider rather than using University Web resources.

v. User posting on official University forums / Social media accounts must be done in a personal capacity and must not contain / disclose any confidential/proprietary information.

System Security Policy

1. Security related misuse like breaking security of systems, trying to capture password of other users, damaging/gaining access to the data of the other users is taken most seriously.

Registrar
Swami Rama Himalayan University

2. Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate. Depending upon the nature of the violation, the university authorities may fine/or and take an action by issuing a warning through disabling the access. In extreme cases, the access to the network may be completely disabled to IT facilities at Swami Rama Himalayan University, and/ or sent to the University disciplinary action committee as constituted by the University authorities.

3. 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.

Internet usage Policy

Prohibited Downloads

The following downloads are specifically not allowed on computers unless approved in writing by Central IT:

a) Any peer to peer file sharing application: Such applications may be used to utilize bandwidth inappropriately. Further, these applications contain third-party applications called adware or spyware, that collect information about a user's Web surfing habits, change system settings, or place unwanted advertising on the local computer.

b) Any third party personal antivirus or firewall: Since adequate security has already been provided for on all machines via pre-defined firewall rules, third party firewalls may interfere with these rules thus endangering the network.

c) Any third-party screen saver or wallpaper: This is to prevent images that might be deemed offensive by some users from being displayed on monitors. Users should use the default screen savers available on their local machines.

d) Hacking tools of any sort: The use of any such tools on University machines is strictly prohibited.

e) Games & Movie trailers or previews: These provide no productive academic benefit and have a tendency to affect productivity, and hence are not allowed on University machines. Users who use their own local machines / University provided portables on which to work are exempt from this policy. For this purpose, games could be in any form executable or flash based games downloaded from the Internet.

The Central IT may suspend, block or restrict access to websites, website categories, and content types, file extensions not found suitable for educational environments or not necessary for functionality of university.

Registrar
Swami Rama Himalayan Univers

Network Infrastructure/Routing Policy

i. Users must not attempt to implement their own network infrastructure including, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to Swami Rama Himalayan University IT resources such as modems and virtual private networks (VPNs).

ii. Users must not offer network infrastructure services such as DHCP and DNS. Exceptions to this policy must be coordinated with the local network administrator with prior approval from the Central IT.

iii. Any attempt Re-Routing or Re-NAT network Traffic inside SRHU campus is strictly prohibited.

Encryption policy

University faculty and staff are encouraged to encrypt files, documents, and messages containing sensitive or confidential University information for protection against unauthorized disclosure while in transit.

However, any encryption performed on University systems must use proven standard algorithms and such encryption must permit properly designated University officials, when required and authorized to decrypt the information.

Proven, standard algorithms should be used as the basis for encryption technologies

Encrypted Communications

i. Swami Rama Himalayan University encrypted communications should be stored in the following manner:

   a. The encryption standard used should be 3DES / PGP secured using at least 128 bit encryption.

   b. The decryption keys should be available with the user's supervisor to be used in the event of the data being needed in the absence of the user.

   c. Any use of the decryption key should be with the explicit permission of the Dean / Director or Head of Department.

ii. In general, information should be stored in a decrypted format unless deemed sensitive by the University.

Network Traffic priorities

IT Services can prioritize the types of traffic on the University's Internet and LAN connections.

Registrar
Swami Rama Himalayan University

- classify network traffic into categories based on application, protocol, subnet, Internet location, and other criteria

- provide statistical measurements on the peak and average bandwidth being requested by the above categories

- apply policy based allocation of bandwidth and traffic to protect core University applications and replace less urgent traffic, and

- Provide reports based on the statistics and performance standards.

IT Support Policy:

The IT-Services will provide Technical support and advice on specific IT problems as is possible, but cannot provide full-time computer support for whole range of the devices and activities. IT Support Requests will be prioritize based on given time and resources. Where IT staff are unable to provide specific support, support should be provided based on appropriate maintenance and support contracts or AMC Terms with vendors or suppliers

On Call Telephonic support will be provided for Network Services Only. IT services will provide any hardware or software support to individuals who Log a complaint in Central IT. Any support request will be attended by IT-Staff based on priorities.

Requests for IT support will be prioritized (highest priority first) according to the following categories:

Network Services Infrastructure

Top priority for IT support is the provision of a fast secure network infrastructure. Specific tasks include:

- Monitoring of all network devices in order to detect and respond to faults
- Monitoring of all network traffic using a firewall for network security

- Modifying and extending the network infrastructure. Most work can be carried out in-house. Large rewiring changes use outside contractors.

- Upgrading the existing network infrastructure as and where necessary.

- Adding or modifying the configuration of all devices attached to the network. Users are reminded of the IT rules stating that they must not make or modify network connections without permission from IT support staff.

Registrar
Swami Rama Himalayan University

Administration Network

Second priority for IT support is the provision of the Administration Network, a fileserver to support the department's core administration staff. The Administration Network is fully the responsibility of IT support staff.

Specific tasks include:

- Software and hardware purchasing, installation, and configuration;
- Software and hardware troubleshooting;
- Fileserver and user management;
- Antivirus protection, backup and archiving;
- Advice on software usage and sources of training;

Teaching Laboratories and Lab Classes

Third priority for IT support is provision of the Teaching Laboratories, a fileserver to support the department's core teaching activities. Technical support is mainly the responsibility of IT support staff, however the Teaching Lab Technician can provide limited user support.

Specific tasks include:

- Software and hardware purchasing, installation, and configuration;
- Software and hardware troubleshooting
- Fileserver and user management;
- Antivirus protection and backup;

General Purpose IT Facilities

Fourth priority for IT support is provision of the general purpose IT facilities. IT support staff will cover the following:

- Software and hardware purchasing, installation, and configuration;
- Software and hardware troubleshooting
- Advice on imaging and presentations
- Advice and Configuration of any IT service required for Conferences, Seminars and Events in the University campus.

Personal IT Equipment

Personal Equipment's of Faculty, Staff or Students or any IT equipment not owned by any department of the university is not supported. However, where non-department equipment is being used for department business, then IT staff will carry out an initial assessment and provide advice about how best to resolve the problem. Any assessment or subsequent work carried-out will be scheduled at lower priority than support for department-owned equipment's.

Registrar
Swami Rama Himalayan University

Application and Authentication Standards

University approved Applications and Network services must ensure their programs contain the following security precautions:

a. Should support authentication of individual users, not groups.

b. Should not store passwords in clear text or in any easily reversible form.

c. Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

d. Should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible. Use of Passwords and Passphrases for Remote Access Users

Access to the University Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Policy Enforcement

i. Users found violating this policy may be denied access to University computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal.

ii. Alleged violations will be handled through the University disciplinary procedures applicable to the user.

iii. The University may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability.

iv. The University may suspend, block or restrict access to websites, website categories, and content types, file extensions not found suitable for educational environments or not necessary for functionality of university.

v. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

vi. Any user found to have violated this policy may be subject to disciplinary action found suitable by SRHU authorities, up to and including termination of employment / admission.

Registrar
Swami Rama Himalayan University

Hardware Safety and Security Guidelines

This procedure describes security measures required to protect information assets (and the information that resides on these devices) such as Pc's, notebook or tablet computers,), CD's, flash drives, DVDs, pagers, cell phones or other similar equipment. Each user must follow the requirements for protecting University information.

The practices listed below do not cover all potential risks, but will significantly minimize the likelihood of theft, loss or damage to University equipment and information. They may apply to one type of device and not another; the user is responsible for applying the measures appropriate to the device.

- Make a record of the make and model of the Device and any serial or company identification number on the equipment and store the record in a separate safe place.

- In an office or work area shared with others, or in an area accessible by the public, either secure the device, or keep it with you at all times.

- Back up your data frequently and store the files in a safe location separate from the notebook or other device.

- Encrypt or password-protect each file containing confidential and/or sensitive University information. Make passwords difficult to crack. A mixture of special characters, numbers, and upper and lower case letters is considered the most secure but only if passwords are not stored on the hard disk. If your notebook comes with biometrics software (such as fingerprint imaging) configure the notebook to use it.

- Sensitive and/or Critical information includes, but is not limited to:

    - All information identifiable to an individual (including students, staff, faculty, trustees, donors, and alumni) including but not limited to dates of birth, personal contact information student education records, medical information, benefits information, compensation, loans, financial aid data, alumni information, donor information, and faculty and staff evaluations.
    - The University's proprietary information including but not limited to intellectual research findings, intellectual property, financial data, and funding sources.
    - Information, the disclosure of which is regulated by government
    - Restrict plug and play. Plug and Play is convenient, but can sometimes be dangerous: if someone connects a USB flash drive, MP3 player or external hard disk drive to a notebook, it is recognized automatically and it is then easy to start exporting data.
    - If your notebook is lost or stolen file an FIR with the Police and report the device's serial number as lost or stolen to the IT Service Help Desk.

Registrar
Swami Rama Himalayan University

USER ACCOUNT SECURITY GUIDELINES

a. Be locked out if more than 5 unsuccessful attempted logons
b. Username and password combinations must not be inserted into email messages or other forms of electronic communication unless the message is encrypted.
c. All passwords must be changed at first logon.
d. If an account or password is suspected to have been compromised, report the incident to IT Services and immediately change all of the associated passwords.
e. Users are required to change their passwords periodically.

IT Policy of Swami Rama Himalayan University, Dehradun that has complied with by all its departments in order to maintain availability of information resources for everyone.

Registrar
Swami Rama Himalayan University