SNU IT Acceptable User Policy

Policy # IT301 IT Acceptable User Policy V1.0

SHIV NADAR UNIVERSITY

Release Control

Release Date	Version No:	Details	Released by	Approved by
12.11.2013	V0.3	Pre Release, the purpose of pre-release is to inform all stake holders about the issuance of this policy and also to give advance intimation to the assured departments to get prepared. The policy will be released after 3 business days of pre-release.	Sunita Surpur	Anand Padmanabhan
05.12.2013	V1.0	First Release	Sunita Surpur	Anand Padmanabhan

POLICY ASSURED BY:

Department:	Represented By:	Date
IT Services (Policy Owner)	Joyjit Roy Ghatak Choudhury	05.12.2013
CIO	Anand Padmanabhan	05.12.2013

POLICY RATIFIED BY:

Office of:	Represented By:	Date
Registrar SNU	Samuel Ernest	05.12.2013
Director School of Engineering	Madan Gopal	05.12.2013
Director School of Humanities & Social Sciences	Shubhashis Gangopadhyay	05.12.2013
Director School of Management and Entrepreneurship	Shekhar Chaudhuri	05.12.2013
Director School of Natural Sciences	Rupamanjari Ghosh	05.12.2013
President SNU	Rajiv Swarup	05.12.2013
Vice Chancellor SNU	Nikhil Sinha	05.12.2013

Table of Contents

HEADING	PAGE
OBJECTIVE	4
SCOPE	4
YOUR RIGHTS AND RESPONSIBILITIES	5
POLICY DETAILS	5
ACCEPTABLE USE	5
FAIR SHARE OF RESCOURCES	6
ADHERENCE WITH CENTRAL, STATE, LOCAL, CYBER AND APPLICABLE INTERNATIONAL LAWS	7
OTHER INAPPORPRIATE ACTIONS	8
PRIVACY AND PERSONAL RIGHTS	8
PRIVACY IN EMAIL	8
ENOFORCEMENT	8
USER COMPLIANCE	9

Policy Details

1. OBJECTIVE

The computing resources at Shiv Nadar University (SNU) support the educational, instructional, research and administrative activities of the University and the use of these resources is a privilege that is extended to members of the SNU community. As a user of these services and facilities, you have access to valuable University resources, sensitive data and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. Individuals need to comply with the Acceptable Use Policy at all times. Individuals are also subject to central, state, local, cyber and applicable international laws governing many interactions that occur on the Internet. Applicability of these laws will change in line with amendments made in these laws as incorporated by their respective governing bodies.

This document establishes specific requirements for the use of all computing and network resources at SNU.

2. SCOPE

This policy applies to all users of computing resources owned or managed by SNU. Individuals covered by the policy include (but are not limited to) permanent and visiting faculty, staff, students, alumni, guests or agents of the administration, external individuals and organizations accessing network services via central computing facilities.

Computing resources include all university owned, licensed or subscribed and leased or managed software and hardware 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.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments (such as the University Libraries and Information Technology Services), personally owned computers and devices connected by wire or wireless to the University network, and to off-campus computers that connect remotely to the University's network services.

2.1. YOUR RIGHTS AND RESPONSIBILITIES

As a member of the University community, the University provides you with the use of scholarly and work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a faculty or staff member or a matriculated student), and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. You are 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.

As a representative of the SNU community, you are expected to respect the University's good name in your electronic dealings with those outside the University. Effective security is a team effort involving the participation and support of every member of the University who deals with information or information systems. It is the responsibility of every computer user to know applicable guidelines, and to conduct their activities accordingly.

3. POLICY DETAILS

3.1. ACCEPTABLE USE

The below list provides a framework for activities which are in the category of acceptable use.

3.1.1. You should only use the computers, computer accounts, and computer files for which you have authorization.

3.1.2. You should not use another users' account or attempt to capture or guess other users' passwords.

3.1.3. You are individually responsible for appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. Therefore, you are accountable to the University for all use of such resources. As an authorized SNU user of resources, you should not enable unauthorized users to access

the network by using a SNU computer or a personal computer that is connected to the SNU network.

3.1.4. The University is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources. You can't violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulation as this will qualify as illegal downloading. Also installation or distribution of "pirated" or other software products that are not appropriately licensed for use is strictly prohibited.

3.1.5. You should make reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing SNU's network and computing resources.

3.1.6. You should not 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.

3.1.7. You should comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

3.1.8. You should not use SNU computing or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

3.1.9. On SNU network or computing systems, you should not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized to do so by the Chief Information Officer (CIO), SNU.

3.2. FAIR SHARE OF RESOURCES

Information Technology Services, and other University departments which operate and maintain computers, network systems and servers, are expected to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade

performance for others. The campus network, computer clusters, mail servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the SNU community is explicitly forbidden.

The University may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

3.3. ADHERENCE WITH CENTRAL, STATE, LOCAL, CYBER AND APPLICABLE INTERNATIONAL LAWS

As a member of the SNU community, you are expected to uphold local ordinances and central, state, cyber and applicable international laws. SNU guidelines related to use of technologies derive from this concern, including laws regarding license, copyright and the protection of intellectual property. As a user of SNU's computing and network resources you must:

3.3.1. Abide by all Central, State, Local, Cyber and applicable International Laws.

3.3.2. Abide by all applicable copyright laws and licenses. SNU has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.

3.3.3. Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information as the ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.

3.3.4. You should not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

3.3.5. You should not use SNU computing and network resources for illegal activities.

3.4. OTHER INAPPROPRIATE ACTIVITIES

Use SNU's computing facilities and services for those activities that are consistent with the educational, research and public service mission of the University. Other prohibited activities, but by no means exhaustive, include:

- Activities that would jeopardize the University's tax-exempt status.
- Use of SNU's computing services and facilities for political purposes.
- Use of SNU's computing services and facilities for personal economic gain.

3.5. PRIVACY AND PERSONAL RIGHTS

3.5.1. All users of the University's network and computing resources are expected to respect the privacy and personal rights of others.

3.5.2. You should not access or copy another user's email, data, programs, or other files without the written permission of SNU's CIO.

3.5.3. You are expected to be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to disciplinary action by University as well as legal action by those who are the recipient of these actions.

3.5.4. Privacy in Email: While every effort is made to insure the privacy of SNU's email users, this may not always be possible. In addition, since faculty and staff members 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 authorized offices, reserves and retains the right to access and inspect stored information without the consent of the user.

3.6. ENFORCEMENT

For security and network maintenance purposes, authorized members within IT services can monitor equipment, systems and network traffic, at any time. IT services reserves the right to audit networks and systems, as required to ensure that SNU is not subject to claims of institutional misconduct and for determining if an individual is in violation of this policy. If an individual is found to be in violation of this policy, the University will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University.

You can report any violations of the Acceptable Use Policy to IT Services at helpdesk@snu.edu.in.

Access to files on University-owned equipment or information will only be approved by specific members when there is a valid reason to access those files. Authority to access user files can only come from the CIO in conjunction with the Vice Chancellor, President, Dean of Student Welfare and/or legal department. External law enforcement agencies and Public Safety may request access to files through valid subpoenas and other legally binding requests. All such requests must be approved by the President in conjunction with the legal department. Information obtained in this manner can be admissible in legal proceedings or in a University hearing.

3.7. USER COMPLIANCE

When you use University computing services, and accept any University issued computing accounts, you agree to comply with this and all other computing related policies. You have the responsibility to keep yourself up-to-date on changes in the computing environment, as published, using either University electronic or print publication mechanisms, and to adapt to these changes as necessary.