SRINIVAS UNIVERSITY

SAMAGRA GNANA

SRINIVAS UNIVERSITY

(PRIVATE UNIVERSITY ESTABLISHED UNDER KARNATAKA STATE ACT NO.42 OF 2013)
City Office : G.H.S. Road, MANGALURU - 575 001. Karanataka State, INDIA.
Phone No.:0824-2425966, 2444891, Fax : 0824 - 2442766
E-mail:info@srinivasuniversity.edu.in website:www.srinivasuniversity.edu.in

Office of the Registrar
SU/REG/F-112/2017

Date: 22/04/2017

Name of the Policy/ Guidelines	**Information Technology Policy**
Short Description	Policy and Guidelines on the use of Information Technology in Education and Governance
Scope	This Policy is applicable to all Teaching, Non-Teaching, Staff, Students, Research scholars, and Administrator of the Constituent Units and Departments of Srinivas University
Policy status	Original
Date of approval of Original Policy	22.04.2017
Effective date	22.04.2017
Approval Authority	Board of Management
Responsible officer	Registrar

Registrar

REGISTRAR
SRINIVAS UNIVERSITY
MANGALORE

INTRODUCTION

With digitization pervading into every facet of our life, we are witnessing an unprecedented need for internet. Further, to increase productivity by reducing monotony of duplication, IT enabled services have become indispensable requisites in educational institutions and research organizations. Realizing the importance of these services, Srinivas University took the initiative way back in year 2009 to establish basic network infrastructure for the IT department in the academic complex at Srinivas University assigning it with the responsibility of running the Srinivas University intranet and Internet services. The IT Section manages the firewall security, proxy, DHCP, DNS, E-mail, web and application servers and the network of the Srinivas University.

NEED FOR IT POLICY

In the absence of clearly defined IT policies, it is difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users.

Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires. Hence, policies and guidelines form the foundation of the Institution's security program. Effective policies are a sign of due diligence; often necessary in the event of an IT audit or litigation.

Policies also serve as blueprints that help the institution implement security measures. Aneffective security policy is as necessary to a good information security program as a solid foundation. Hence, Srinivas University also is proposing to have its own IT Policy that works as guidelines for using the Srinivas University's computing facilities including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called as **"Srinivas University Information Technology Policy".** This document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of the Srinivas University.

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of the information technology policies that govern information, security processes are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

OBJECTIVES OF THE POLICY

1. To maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the Srinivas University on the campus.
2. To outline Srinivas 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 Srinivas University.

SCOPE & JURISDICTION

It may be noted that IT Policy of Srinivas University applies to technology administered by the Srinivas University centrally or by the individual departments, to information services provided by the Srinivas University administration, or by the individual departments, or by individuals of the Srinivas University community, or by authorised resident or non-resident visitors on their own hardware connected to the Srinivas University network. This IT policy also applies to the resources administered by the central administrative departments such as library, computer centers, laboratories, offices of the Srinivas University recognised associations, or hostels and guest houses, or residences wherever the network facility was provided by the Srinivas University.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the IT policy of Srinivas University. Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the Srinivas University information technology infrastructure, must comply with the guidelines. Certain violations of IT policy laid down by the Srinivas University by any member may even result in disciplinary action against the offender by the Srinivas University authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

This Policy Applies to all Stake Holders and resources of Srinivas University, its Institutes, Units and Hospitals as detailed below:

A. Stakeholders coming under the purview of the following establishments are covered underthis policy

1. Institute Of Engineering and Technology
2. Institute Of Management & Commerce
3. Institute Of Allied Health Sciences
4. Institute Of Computer Science & Information Science
5. Institute Of Social Sciences & Humanities
6. Institute Of Hotel Management & Tourism
7. Institute Of Physiotherapy
8. Institute Of Education
9. Institute Of Nursing Science

B. Stake holders on campus or off campus includes

Students: UG, PG, Research Administrative Staff (Non-Technical /Technical) Employees (Permanent/ Temporary/ Contractual) Higher Officers Faculty Guests

C. Resources Include

Network Devices wired/wireless Data Storage Wi-Fi Network Mobile/ desktop / server computing facility Internet Access Multimedia Contents Official Websites, web applications Documentation facility (Printers/Scanners) Official Email services further, the policies will be applicable at two levels:

- End Users Groups (Faculty, students, senior officers, administrative staff (both teaching and non-teaching) and other employees
- Network administrators

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organisation, departments and individuals who are part of Srinivas University community to understand how Srinivas University policy applies to some of the significant areas and to bring conformance with stated policies.

Broadly Speaking the IT Policy of Srinivas University stands not only for IT asset security and safety but also for the responsible use of IT facilities by the users of Srinivas group of education.

It is to be noted that IT Policy of Srinivas University is formulated and executed in consonance with service rules of Srinivas University.

The Board of Management of the Srinivas University will have the power to interpret the IT policy of Srinivas University and the same shall be implemented by Vice chancellor of Srinivas University. Systems Administrator shall receive the complaints regarding IT issues and the Registrar - Srinivas University shall be the competent authority to take necessary actions regarding complaints and disciplinary actions in case of any misconducts. The said disciplinary action shall be initiated/taken by Registrar after approval from the Board of Management. Heads of the Institute/ Units/ Departments upon the report from point of contact shall have the power to give complaints to Registrar through Assistant Director- HR or Systems Administrator of Srinivas University Regarding IT Issues/ problems.

However initially, as the IT literature among the employees of establishment is complex due to dynamic nature of information technology and varied superior subordinate relationship, Systems Administrator takes the responsibility of policy execution in step by step mode at each level, after obtaining due approval from the competent authority.

Policy Supporting Documentation	**Policy Support Contact**
Service and Conduct Rules Srinivas University	Systems Administrator Srinivas University

SECTIONS OF POLICY DOCUMENT:

1. Hardware Installation
2. Software Installation and Licensing
3. Web Site Hosting
4. Acceptable Use, Internet/Network (Intranet and Internet) Use
5. Acceptable Use, Email /E-mail Account Use
6. Srinivas University Database Use and Information Dissemination
7. Access Controls, Use Accounts
8. Data Privacy
9. Protection against Computer virus and malware
10. Cyber Security
11. Data Backup, Storage and recovery
12. General Information Security Management
13. Responsibilities of IT Department
14. Responsibilities of the Administrative Units
15. Guidelines on Computer Naming Conventions
16. Guidelines for hosting Web pages on the Internet/Intranet
17. Guidelines for Desktop Users
18. Green Computing
19. Video Surveillance

SRINIVAS UNIVERSITY
SRINIVAS NAGAR
MUKKA
SURATHKAL
574 146
MANGALORE

- **HARDWARE INSTALLATION**

Network user community of Srinivas University 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.

Who is primary user?

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

What are end user computer systems?

Apart from the client PCs used by the users**,** the Srinivas University will consider servers not directly administered by IT department, 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 IT department, are still considered under this policy as "end-users" computers.

Power connection to computers and peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

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.

File and print sharing facilities

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

Shifting computer from one location to another

Computer system may be moved from one location to another with prior written intimation to theIT Department as IT department maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room number. As and when any deviation (from the list maintained by IT Department) is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs IT department in writing/by email, connection will be restored.

Replacement of equipment

In general, ICT equipment should not be replaced until it fails, is uneconomical to repair or becomes unusable. The latter would generally occur when the equipment can no longer run the software or operating system at all, or at a reasonable, productive speed.

Although the standard manufacturer warranty for computer hardware is three or five years in General. For laptops, users are advised to buy extended manufacturer warranties.

As desktop equipment is part of the ICT infrastructure used to deliver a range of core services, ICTS may, from time to time, issue notices that certain equipment should or must be replaced.

SRINIVAS UNIVERSITY
SRINIVAS NAGAR
MUKKA
SURATHKAL
574 146
MANGALORE

This may occur prior to the recommended replacement periods below.

a. Desktop Computers
Desktop computers may not be replaced before the end of a 7 year cycle.

b. LCD Monitors
The expectation is that LCD monitors will last at least 8 to 10 years. Replacement is to be based on failure and is not bound to a particular cycle.

c. Second machines, tablets and laptops
A staff member who has a laptop or desktop may be provided with a tablet where good cause is shown; however, where a staff member has a thin/light laptop there may be no justification fora tablet. Laptops may not be replaced before the end of a 7 year cycle.

d. Computer accessories
Computer accessories such as keyboards, mice, stands and related accessories should be replaced on failure and are not bound to a particular cycle.

e. Printers
Staff members must print to department/central printers whenever possible due the lower cost per page. Desk-based printers may be deployed only where a clear need exists and the purchase of ink jet printers should be avoided due to their higher operating costs.

f. Disposal of replaced hardware
If ICT equipment cannot be re-deployed internally, then the processes as recommendedby the Disposal of IT equipment policy must be followed. It is important that the disposal satisfies audit requirements, and is undertaken in the most economically advantageous manner.

g. Each student should purchase a suitable Laptop Computer as per their Course requirements of the Programme. The University will provide Wi-Fi based Internet facility for these laptop computers. Accordingly, the course fee is kept low.

h. As per UGC & AICTE guidelines, Srinivas University promoted Open Access Software in its curriculum and laboratories wherever possible.

Provision for standby equipment

When a Desktop computer, laptop or printer breaks down, on request of the concerned department's Head, the IT department will provide the standby desktop available at their disposal. The request should come in the official email to the IT department. The issue and receipt of the equipment will be made through official email communication. Inventory information is updated at both the departments. The IT department will install required licensed software with help of the concerned department.

The concerned department which received the standby ICT equipment will inform and return the device, when its equipment gets repaired. The IT department will coordinate with the designated vendors to repair the device and will certify the repair charges after obtaining the user feedback.It also makes sure that Vendor has taken sufficient care of the privacy of the data and equipment itself while repairing.

Power back-up for hardware installations

The continued and uninterrupted operation of the Srinivas University's Information and Communications Technology (ICT) equipment, servers at Data centre and network equipment is essential to the mission of the university. Towards this end, the university will maintain a two tiered power back-up - (1) diesel generators and a 20-kilowatt uninterruptible power system (UPS). The purpose of this policy is to set forth guidelines for the operation, testing, and maintenance of these systems.

The Backup Power systems are designed to operate without significant manual intervention. They will start automatically when an interruption of electrical power from the utility power grid is detected and will continually operate until the power is restored. Normally, the only operational tasks required are to monitor the level of diesel fuel in the tank and to observe the scheduled automatic tests of the systems.

The protected network and server equipment in the Data Centre draws its power from the UPS at all times, even when commercial power is available. The batteries are continuously recharged from this commercial power. When an interruption of electrical power from the commercial power grid is detected, the equipment which is connected to the UPS will continue to operate from the UPS with no interruption in service, but the generator will automatically start up to provide power to recharge the batteries. When the commercial power is restored and has becomestable, the electrical service switches back to the commercial power grid and the generator shuts down automatically. The equipment protected by the Backup Power System UPS includes all servers in the Data Centre, essential network equipment, the telephone switchboard, the Help Desk, and the building access and alarm system.

In addition, Faculty/student used computers will be provided with small UPS which provide power during power supply changeover between grid and generator.

Testing at a predetermined time and day in each week, the generator will automatically startand will run for an interval long enough to warm up the oil.

Maintenance

The systems are initially under full warranty. Upon the expiration of those warranties, a maintenance agreement will be negotiated with the appropriate electrical contractors. UPS batteries are replaced at regular intervals.

General user responsibilities

ICT equipment located in common or open areas, and in computer labs must be secured with an approved security solution, such as a cable and lock. When unoccupied, rooms should be locked and alarmed. Similarly, staff should appropriately secure their equipment and offices.

Most pieces of ICT equipment contain sensitive electronic components that can be adversely affected byshock, heat, dust and liquid. Equipment should be located off the floor, preferably ona sturdy surface, away from direct sunlight and other heat sources, and situated such that other objects (i.e. books, papers, furniture) do not block the cooling vents.

Food and drink should always be kept away from any computer equipment. Most equipment can be safely dusted off with compressed (canned) air and wiped with a soft cloth slightly dampened with water only. Equipment should be turned off prior to cleaning or moving.

Non compliance

Faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole Srinivas University . Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

IT department interface

IT Department upon finding a non-compliant computer affecting the network, will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the IT Department, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The IT Department will provide guidance as needed for the individual to gain compliance.

➢ SOFTWARE INSTALLATION AND LICENSING POLICY

Anti-Piracy measures

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

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

Operating system and its updating

Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

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

Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is user's responsibility to make sure that the updates are being done properly.

Antivirus software and its updating

Computer systems used in the Srinivas 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.

He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the user's technical skills, the user is responsible for seeking assistance from IT department.

Backups of data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C driveand user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a fool proof solution. Apart from this, users should keep their valuable data either on floppy, or CD or other storage devices such as pen drives as approved by IT department of Srinivas University.

Service arrangements

In order to meet the needs of the University stake holders, some services will need to be outsourced to third parties. In such cases, the University mandates a Service Level Agreement (SLA) for all software and hardware related services in addition to issue of work orders with detailed terms and conditions. Service Level Agreements will list out expectations and quality ofthe service. It also provides remedies if service requirements are not met.

The SLA should include not only a description of the services to be provided and their expected service levels and quality, but also metrics by which the services are measured, the duties and responsibilities of each party, the remedies or penalti5es for breach, and a protocol for adding and removing metrics Faculty or university institution may take the help from the Legal department and Purchase department while formulating the draft and finalising the same considering all the factors relatedto Technology, Privacy protection, Finance and Legal issues. The service level agreement should comply with the rule of the land.

Non compliance

Srinivas University faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files, inoperable computer resulting in loss of productivity, risk of spread of infection to other users, confidential data being revealed to unauthorized persons. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, Departments, or even whole Srinivas University. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

➢ WEB SITE HOSTING

Official pages

Sections, departments, and associations of teachers/employees/students may have pages on intranet channel of the official web page of Srinivas University. Official web pages must conform to the Srinivas University web site creation guidelines for web site hosting. As on date, the Srinivas University's IT department is responsible for maintaining the official web site of the Srinivas University, viz., https://srinivasuniversity.edu.in/

If department wants to have a page related to their department activity they may request IT department.

Web pages for E-learning:

Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the web linked through the appropriate department's pages.

Because majority of student pages will be published on the Srinivas University 's Web for E Learning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official Srinivas University or other web sites. If a student publishes a fictional web site or a web site modelled after an existing institution or corporation, the site must be clearly identified as a class project.

The following are the storage and content requirements for class-generated student web pages:

A) Servers:

It is recommended that pages be placed on the student information server, but pages developed for classes also may be placed on departmental servers or the main campus server meant for E learning purpose.

B) Maintenance:

If the pages are published on the E- learning information server, they will be maintained under the default rules for personal E-learning pages.

The instructor will maintain pages that are published on departmental servers or the main campus server meant for E-learning purpose.

C) Content disclaimer:

The home page of every class-generated site will include the Srinivas University Content Disclaimer (for pages published on the E-learning information server, the content disclaimer should be generated automatically)

D) Official pages:

If web pages developed for E-Learning become the part of the "official" Srinivas University page, they must be removed from the E-learning information server, departmental servers as class-generated pages (students, can of course, link to their work from their personal student pages).

➢ INTERNET/NETWORK (INTRANET AND INTERNET) USE

Overview and Purpose

The internet provides a source of information that can benefit every professional discipline represented in the Srinivas University. This policy document delineates acceptable use of internet capabilities by Srinivas University employees, volunteers, and contractors by means of equipment, facilities, internet addresses, or domain names owned, leased, or registered to Srinivas University.

Network connectivity provided through the Srinivas 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 IT Policy of Srinivas University. The IT Department is responsible for the ongoing maintenance and support of the network, exclusive of local applications. Problems within the Srinivas University's network should be reported to IT department.

Coverage

Anyone who uses Srinivas University equipment and facilities, and performed using internet protocol addresses and domain names registered to Srinivas University. This includes, but is not limited to:

- Full and part time employees
- Volunteers authorized to use Srinivas University resources to access the internet
- Departmental contractors authorized to use Srinivas University equipment or facilities

All content that resides on or passes through Srinivas University Information Resources, including computers, networks, and software, must conform to the Srinivas University acceptable use Internet policy. This policy applies to internet access only. It does not cover the requirements, standards, and procedures for the development and implementation of Srinivas University' s information sites on the internet.

Roles and Responsibilities

A. Supervisors

Supervisors of employees, volunteers, and contractors have the final authority in determining whether an employee requires internet access to fulfil job requirements. Supervisors are responsible for:

- Acquiring internet access for subordinate employees, as needed.
- Educating subordinate employees on restrictions against personal use of Srinivas University networks, systems, and other electronic resources.
- Determination of appropriateness of subordinate employees' use of the internet. This includes judgment of the acceptability of internet sites visited and the determination of personal time versus official work hours.

B. System users

Use of computer equipment and networks to fulfil job responsibilities always has priority over personal use of equipment and networks. In order to avoid capacity problems and to reduce the susceptibility of Srinivas University information technology resources to computer viruses and other malware, all internet users must:

- Follow all security policies and procedures covering use of internet services.
- Refrain from any practice that might expose, compromise, or otherwise jeopardize organizational networks, computer systems, data files, and other electronic resources.
- Understand legal requirements and limitations regarding access, protection, and use of data covered by the "National Privacy Act", copyright law, trademark law, and internal policy.

IP address allocation:

Any computer (PC/Server) that will be connected to the Srinivas University network, should have an

IP address assigned by IT department. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building 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 unauthorised from any other location. As and when a new computer is installed in any location, the concerned user can download the application form available for the purpose of IP address allocation and fill it up and get the IP address from the IT department.

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. IP addresses are given to the computers but not to the ports. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

DHCP and proxy configuration by individual department's /sections/ users:
Use of any computer at 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 absolute violation of IP address allocation policy of the Srinivas University. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the servicerun by IT Department. Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.
Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned user. Also it may be reported to HR department for disciplinary action.

Running network services on the servers:

Individual departments/individuals connecting to the Srinivas 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 IT department in writing and after meeting the requirements of the Srinivas University IT policy for running such services. Non-compliance with this policy is a direct violation ofthe Srinivas University IT policy, and will result in termination of their connection to the network.

IT department takes no responsibility for the content of machines connected to the network, regardless of those machines being Srinivas University or personal property. IT department 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. Access to remote networks using a Srinivas 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 Srinivas University Network connects. Srinivas University network and computer resources are not to be used for personal commercial purposes. Network traffic will be monitored for security and for performance reasons at IT department. Impersonation of an authorized user while connecting to the network is in direct violation of this agreement and will result in the termination of the connection and disciplinary action.

Broadband connections:

Computer systems Using USB Dongles that are a part of the Srinivas University 's campus-wide network, whether Srinivas University 's property or personal property, should not be used for broadband connections, as it violates the Srinivas University 's security by way of by-passing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

Wireless local area networks:

A. This policy applies, in its entirety, to department or units wireless local area networks. In addition to the requirements of this policy, departments or units must register each wireless access point with IT department including point of contact information.

B. Departments/ units must inform IT department for the use of radio spectrum, prior to implementation of wireless local area networks.

C. Departments/ units must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.

Internet Bandwidth obtained by other departments:

Internet bandwidth acquired by any section, department of the Srinivas University under any research Programme/project should ideally be pooled with the Srinivas University's internet bandwidth, and be treated as Srinivas University's common resource.

Under particular circumstances, which prevent any such pooling with the Srinivas University's internet bandwidth, such network should be totally separated from the Srinivas University's campus network. All the computer systems using that network should have separate IP address scheme (private as well as public) and the Srinivas University's gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the Srinivas University's 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 IT department.

A. Internet Access

If an employee's supervisor determines that Internet access is in the best interest of Srinivas University, the employee may, within the limits set forth below, use Srinivas University networks and equipment to access the internet. Employees who do not require access to the Internet as part of their official duties, may not access the internet using Srinivas University's facilities under any circumstances.

B. Permitted Use

- Access to online job related information, as needed, to meet the job requirements.
- Participation in newsgroups, chat sessions, email communications, and online discussion groups, provided those communications activities have direct relationship to the user's job responsibilities.
- Access to online content to develop or enhance job related skills. It is expected that these skills will be used to improve the accomplishment of job related work assignments.

C. Use of internet and company networks for non-business purposes

Srinivas University's computer systems are for official and educational use; However, when certain criteria are met, departmental users may use information resources for personal activities. All personal internet use through business information resources are subject to the following restrictions:

- They must not degrade or otherwise impede normal job performance
- They do not incur direct costs to Srinivas University

Since employees who use Srinivas University's information resources may be perceived by others to represent Srinivas University, employees may not use the internet for any purpose that could reflect negatively on Srinivas University or its employees. Personal opinions expressed over the course of online communications activities should include a disclaimer stating that they do not reflect official positions of Srinivas University.

Employees may not initiate non work related internet sessions using Srinivas University information resources from remote locations. For example, employees shall not log into organizational resources from home or other remote locations to engage in non-job related activities. Personal use of Srinivas University's Information Resources to access the Internet is restricted to approved users; It does not extend to family members or other acquaintances.

D. Reasonable security and privacy precautions

- All files downloaded from the internet must be scanned for viruses using approved software andcurrent virus detection software.
- Any corporate data posted on internal web sites must not be available to access by a broader online audience than is appropriate for the materials themselves.
- All sensitive business materials transmitted over external networks must be encrypted.
- No files or documents may be sent or received that may cause legal liability for, orembarrassment to the Srinivas University.

E. Use of internet client and browser software

- All software used to access the internet must be part of the Srinivas University standardsoftware suite orapproved by IT management.
- IT staff must update Internet clients and browsers as vendor provided security patches are released.
- Internet clients and browsers must be configured to use the Srinivas University firewall http proxy.

F. Prohibited use

Employees may not use Srinivas University's information resources, either during working hours or onpersonal time, to:

i. Access, retrieve, or print text and graphics information that violate the acceptable use policy
ii. Engage in unlawful activities or other activities that could in any way discredit Srinivas University
iii. Engage in personal commercial activities, including offering services or merchandise for sale, non-business related online purchasing, and personal commercial advertising. Where online commercial transactions are permitted as part of legitimate job functions, transactions aresubject to Srinivas University's procurement rules.
iv. Engage in any activity that would compromise the security of Srinivas University 's systems, resources, or networks
v. Engage in any fund raising activity, endorse any product or services, participate in any lobbying activity, or engage in any active political activity
vi. Access or download video and voice from the internet, except in the service as an approved job function.
vii. Store personal files obtained via the Internet on Srinivas University 's drives, servers, or other devices

G. Enforcement

i. All activity on Srinivas University's information resources is subject to monitoring by management, H.R personnel, system and security personnel, legal personnel, and other authorized staff. Monitoring includes logging and review. Use of Srinivas University's systems constitutes consent to monitoring.
ii. All files and documents—including personal files and documents—stored on or transmitted by company information resources are subject to managerial review and may be accessed inaccordance with this policy.
iii. Violation of this policy may result in disciplinary action, including termination for employees and temporaries; A termination of employment relations in the case of contractors or consultants; Dismissal for interns and volunteers; Or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Srinivas University's information resources access privileges, civil, and criminal prosecution.

Non-compliance to this policy will be direct violation of the Srinivas University's IT security policy.

SRINIVAS UNIVERSITY
SRINIVAS NAGAR
MUKKA
SURATHKAL
574 146
MANGALORE

➤EMAIL/EMAIL ACCOUNT USE

Overview and Purpose

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the Srinivas University's administrators, it is recommended to utilize the Srinivas University's e-mail services, for Srinivas University's formal communication and for academic and 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 Srinivas University communications are official notices from the Srinivas University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Srinivas 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 **https://srinivasuniversity.edu.in/** with their **User ID** and **password**. For obtaining the Srinivas University's email account, user may contact IT department for email account and default password by submitting an application in a prescribed format through head of the institute/units.

The Srinivas University's electronic mail (email) facility offers employees and contractors an efficient way to communicate with others inside, and outside (via Internet) the Srinivas University using the organization's computer systems. The purpose of this policy is to:

- Establish rules for the creation and transfer of information through the Srinivas University's internalemail system.
- Prevent unintended disruption or degradation of network communications and the efficientoperations of email systems.

Coverage

All individuals authorized to use any Srinivas University's information resource with the capacity to send, receive, or store electronic mail.

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

i. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes. I.e. Srinivas University employees may make incidental personal use of email but any incidental email usage for personal use may not interfere with official duties, must have a minimal effect on the organization, and must be consistent with official duties, must have minimal effect on the organization, and must be consistent with standards of ethical conduct.

ii. Using the facility for illegal/ commercial purposes is a direct violation of the Srinivas 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, sending of unsolicited bulk e-mail messages and generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

iii. Authorized Srinivas University email users are not permitted to forward Srinivas University email or attachments to personal accounts managed by public email or internet access service providers where the information might be compromised.

iv. Srinivas University employees and contractors are not authorized to use the email system to send sensitive information via the internet where information might be intercepted.

v. System Users must must not send, forward, receive or store confidential or sensitive Srinivas University information utilizing non Srinivas University accredited mobile devices. Examples of mobile devices include, but are not limited to, personal data assistants (PDAs), two way pagers, tablets and cellular telephones.

vi. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.

vii. User should not open any mail or attachment that is from suspicious/ unknown source. Even ifit is from known source, and if it contains any attachment that is of suspicious nature or look dubious, 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 potential to damage the valuable information on your computer.

viii. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.

ix. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

x. While Using the computers that are shared by other user 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 hasoccupied that computer for its use.

xi. Impersonating email account of others will be taken as a serious offence under the Srinivas University's IT security policy.

xii. It is ultimately each individual's responsibility to keep their e-mail account free from violations of Srinivas University's email usage policy.

xiii. All the mails detected as Spam mails go into SPAM MAIL folder of the respective user's 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.

xiv.The above laid down policies particularly 1 to 12 are broadly applicable even to all the email services that are provided by other sources, as long as they are being used from the Srinivas University 's campus network, or by using the resources provided by the Srinivas University to the individual for official use even from outside.

B. Appropriate use of email

Appropriate use of the Srinivas University email system includes generating and sending emailsregarding:

- Srinivas University 's mission and program related activities
- Other related and endorsed activities with respect to Srinivas University
- Subject to the limitations contained in this email policy statement, brief occasional personal messages

C. Inappropriate use of email

Srinivas University email facility may not be used to:

- Send email intended to intimidate or harass individuals or organizations
- Conduct personal business
- Send unsolicited messages to large groups, except as required to conduct organizational business
- Sending excessively large messages or messages with attachments larger than 20mb
- Send or forward email that is likely to contain computer viruses
- Sending or forward personal messages to everyone in the company directory or other large user groups
- Send or forward chain letters
- Conduct political lobbying or campaigning
- Violate copyright laws by inappropriately distributing protected works

D. Email system users may not:

- Represent themselves as anyone other than themselves when sending email, except when explicitly authorize to do so in an administrative support role.
- Use unauthorized email software
- All sensitive Srinivas University material transmitted over external network must be encrypted.
- Email system users must not give the impression that the user is representing or making statements on behalf of Srinivas University, except under condition of explicit authorization.

- The following disclaimer must be included in all messages sent through the email system: "The opinions expressed in this message are my own, and not necessarily those of my employer."
- For other terms and criteria of system use, refer to the organization's policy on acceptable use: internet.

E. Enforcement

- All activity on Srinivas University 's information resources is subject to logging and review
- If an inappropriate email is brought to our attention, the sender may be directed by either the email postmaster or the computer security officer to retract the message. Inappropriate or unauthorized email may be retracted by the postmaster if the sender is not available.
- Violation of this policy may result in disciplinary action, including termination for employees and temporaries; A termination of employment relations in the case of contractors or consultants; Dismissal for interns and volunteers; Or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Srinivas University's information resources access privileges, civil and criminal prosecution.

➤ **SU - IT & Computer policy**

- Each student should purchase a suitable Laptop Computer as per their Course requirements of the Programme. The University will provide Wi-Fi based Internet facility for these laptop computers. Accordingly, the course fee is kept low.
- As per UGC & AICTE guidelines, Srinivas University promoted Open Access Software in its curriculum and laboratories wherever possible.
- SU Library Policy Document is also Required and it should also contain following points:
- To the unnecessary cost of SU library and to avoid absolency in Books & Journals, the University promotes Library Collaborations with nearby Universities & HE Institutions thereby contributes to NEP-2020 policy of One Country - One Subscription.
- The Ubiquitous Digital Library (UDL) of Srinivas University has to be expanded continuously by converting all available Physical books into Digital Books with the permission & membership of Petrographic Society of India.
- Through Collaborations and Networking, SU Library provides a copy of any article/chapter of information which is available in open access/ subscription based from any corner of the World to our Stakeholders (students, researchers, staff), in the form of a Soft-copy within 5 days after submission of request letter with applicable fees.

➤ Through Collaborations and Networking, SU library should develop an Ideal system of Information Repository at minimum cost for maximum utilization.

DATABASE USE AND INFORMATION DISSEMINATION POLICY

INTRODUCTION:

This Policy relates to the databases maintained by the Srinivas University administration under the Srinivas University's E- Governance. Data is a vital and important Srinivas University resource for providing useful information. Its use must be protected even when the data may not be confidential. Srinivas University has its own policies regarding the creation of database and access to informationand a more generic policy on data access. Combined, these policies outline the Srinivas University's approach to both the access and use of this Srinivas University's resource.

A) **Database Ownership:** Srinivas University is the data owner of all the Srinivas University's institutional data generated in the Srinivas University.

B) **Custodians of Data:** Individual sections or departments generate portions of data that constitute Srinivas University's database. They shall have custodianship responsibilities forportions of that data.

C) **Data Administrators:** Data administration activities outlined may be delegated to some ofthe officers in that department by the data custodian.

D) **MIS Components:** For the purpose of E Governance, Management Information System requirements of the Srinivas University may broadly be divided into seven categories. Theseare:

(a) Human Resource Information System (HRIS)
(b) Students Information Management System (SIMS)
(c) Financial Information Management System (FIMS)
(d) Asset Tracking/Physical Resources Information ManagementSystem (ATMS)
(e) Library Information Management System (LIMS)
(f) Document Management And Information Retrieval System(DMIRS)

E) **Here are some general policy guidelines and parameters for sections, departments and administrative unit data users:**

(a) The Srinivas University's data policies do not allow the distribution of data that is identifiable to a person outside the Srinivas University.

(b) Data from the Srinivas University's data base including data collected by department or individual faculty and staff is for internal Srinivas University purposes only.

(c) One's role and function define the resources that will be needed to carry out one's official responsibilities/ rights. Through its data access policies, the Srinivas University makes information and data available based on those responsibilities/ rights.

(d) Data directly identifying a person and his/ personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the office of the Registrar- Srinivas University.

(e) Requests for information from any courts attorneys etc are handled by the Registrar's office of the Srinivas University and departments should never respond to requests, even with a writ/court order. All requests from law enforcement agencies are to be forwarded to the office of Registrar - Srinivas University respectively for response.

(f) At no time may information, including that identified as "Directory Information" be released to any outside entity for commercial, marketing solicitation or other purposes. This includes organizations and companies which may be acting as agents for the Srinivas University or its departments.

(g) All reports for UGC, MHRD and other government agencies will be prepared/ compiled and submitted by the Registrar, Controller of Examinations and Finance Officer of the Srinivas University

(h) Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

(i) Tampering of the data base by the department or individual user comes under violation of IT Policy.

A. **Tampering includes but not limited to:**

(j) Modifying/deleting the data items or software components by using illegal accessmethods.

(k) Modifying/deleting the data items or software components deliberately withulterior motives even by authorized individuals/ departments.

(l) Causing database or hardware or system software crash thereby destroying thewhole of orpart of database deliberately with ulterior motives by any individual.

(m) Trying to break security of the database servers.

B. Such data tampering actions by Srinivas University member or outside members will result in disciplinary action against the offender by the Srinivas University authorities. If the matter involves illegal action, law enforcement agencies may become involved in the said matter or issue.

Information Dissemination Policy

A) It should always be kept in mind that the apex custodian for information, data, data base and emails of Srinivas University shall be "The Registrar- Srinivas University". However either it be “internet or intranet', “email or data base”... there will be many information or data which may be disseminated and at the same time there are many information or data on which strict confidentiality may have to be maintained. Respective heads of institute, unit, hospital, department, unit, section... under which such information, emails, data, data base... are maintained shall be its sub custodians.

B) Whenever any information, data, data base or email of Srinivas University is requested or sought by any external person or body (whether it be public/ statutory bodies or private bodies

/persons) such instances should be immediately submitted and brought to the notice of respective custodian (The Registrar- Srinivas University) for further actions on that and further actions on the same shall be carried out either under their approval or authorization.

C) The information or data sought under/through courtorders, summons, notices, shallbe strictly and immediately submitted and brought to the notice of “The Registrar- Srinivas University” for further actions.

➤ ACCESS CONTROLS AND USER ACCOUNTs

Overview and Purpose

Srinivas University must balance employee’s needs to access systems and information with the organizational obligation to control access for the purposes protecting information confidentiality, integrity, and availability. Account passwords are a mainstay of information security controls. This policy establishes management controls for granting, changing, and terminating access to automated information systems, controls that are essential to the security of Srinivas University's information systems.

Coverage

All full and part time employees, contractors, and other personnel who use Srinivas University’s Information Resources, Roles and Responsibilities

A. Systems Administrator

i. Oversees password administration for Srinivas University
ii. Publishes and maintains policy guidelines for the creation, safeguarding, and control of the passwords
iii. Acts as an Information Security Officer (ISO)
iv. Reviews and validates access and rights records at least once per 3 months to confirmcontinuing needfor access
v. Prepares policy guidelines for the creation, safeguarding, and control of passwords
vi. Approves access rights and passwords for privileged accounts for Srinivas University
vii. Issues passwords for privileged accounts.
viii. Issue and manage passwords and account rights for systems and applications under their control

B. Supervisor/ Point of Contact

i. Communicates system access and password requirements to the user community
ii. Informs the Information Security Officer (ISO) if any access or system rights should be changed orremoved
iii. Immediately informs the IT Department if a password is known or suspected to be compromised

C. System users

i. Protect password confidentiality
ii. Immediately notify supervisor if a password is known or suspected to be compromised

D. Password rights administration

i. Access to Srinivas University’s Information resources must be controlled.
ii. Access to Srinivas University’s information resources must be based on an approved system access request form for each discrete system.
iii. Access rights are granted based on the principle of "least privilege": Access is granted only to systems and application necessary for the performance of official duties.
iv. Supervisor /Point of Contact and Systems Administrator (ISO) must approve employee access

rights to Srinivas University information Resources.

v. The Registrar-Srinivas University must approve Supervisor and Systems Administrator to access rights to Srinivas University's Information Resources.

vi. Privileged access passwords (such as those belonging to Systems Administrators) must be changed at least once in every 2 months or when necessary due to employment termination, actual or suspected password compromise.

vii. Information Security Officers and Systems Administrators shall not allow generic or group access credentials, including passwords.

viii. Contractor accounts and access privileges must be terminated on the contract expiration date. Contractor supervisors are required to inform System Administrators of new and changed contract effective dates that are likely to affect account access permissions.

ix. Vendor or service accounts included in acquired software or used for software development must be deleted prior to software deployment.

x. Any default passwords must be changed on all systems prior to connection to any network, even inpre deployment testing.

xi. Administrative account passwords must be changed promptly upon departure of personnel or suspected compromise.

xii. User accounts must be disabled promptly upon departure of personnel. If a user knows or suspects that the confidentiality of their password has been compromised, they must immediately change the password.

E. Password requirement

i. Passwords (login) are required on all Srinivas University's information systems

ii. Each individual users are assigned unique login credentials comprising, at minimum, at unique user name and password

iii. Passwords must conform to the following criteria:

iv. At least eight characters in length

v. Consist of a mix of alpha, numeric, and special characters

vi. Exclude dictionary words

vii. Exclude portions of associated account names (e.g., user ID, login name)

viii. Exclude common sequential character strings (e.g., "abc" or "1234")

ix. Exclude simple keyboard patterns (e.g., "asdf")

F. Automated controls

To reduce the risk that an unauthorized party can gain system access by guessing a user's password, the Srinivas University system(s) shall limit invalid login attempts to three. After three unsuccessful login attempts, the Srinivas University system(s) must automatically "lock out" the attempting user for not less than 1 hour. Note: For critical systems, the policy administrator may wish to specify that "locked out" users must contact a Systems Administrator in order to reactivate a "locked" account.

G. Password protection

i. Users must change passwords immediately after the initial login to any Srinivas University system(s) Information Resource.

ii. Users must not disclose or otherwise allow third party use of their unique account credentials (User IDs and Passwords).

iii. Passwords must be changed at least once in every 2 months.

iv. Passwords may not be reused for at least 5 consecutive login change cycles

v. Passwords must not be embedded in automated programs, utilities, or applications, such as: autoexec.bat files, batch job files, or terminal hot keys.

vi. Passwords must be not rendered in readable form through publicly visible media by any application, printer, web server, or other mechanism.

vii. Passwords must not be stored in readable form in any application, file, or database.

H. Enforcement

Gross negligence or willful disclosure leading to illicit exposure of Srinivas University's informationmay result in prosecution for misdemeanor or felony resulting in fines, imprisonment, civil liability, and/or dismissal.

➢ DATA PRIVACY

This policy section governs users' relationship with Srinivas University regarding the use of the website and its hosted web applications. The university website provides general information regarding the institutions/units and their services. The information available on this website should not be assumed to be complete or up-to-date. The web applications are designed for the university's particular administration.

For third-party developed software/application that deals with student/faculty personal information, University executes a Non-Disclosure agreement (NDA) in the first phase, which is procurement itself. Without NDA, university institutions are not allowed to transfer/provide student/faculty information to any third party.

Privacy Statement

SRINIVAS UNIVERSITY website is operated by the IT department of SRINIVAS UNIVERSITY. Visitors to www.Srinivasuniversity.edu.in are guaranteed privacy. Information collected on https://srinivas university.edu.in is kept private and never shared with other organizations.

Measuring Audiences

User IP (Internet Protocol) address is used to gather broad demographic information. SRINIVAS UNIVERSITY logs IP addresses and browser types for systems administration purposes. These logs are analyzed constantly to improve the value of the materials available on this website. The IP address also helps us diagnose problems with the university's server and administer the website. IP addresses do not provide us with any identifiable personal information. This means users' sessions will be tracked but will remain anonymous to us in case of the website does not require a login to view the information.

Cookies

To better understand the way our websites are used by visitors, SRINIVAS UNIVERSITY employs the use of cookies, a small file that stores information on users' hard disk drives. SRINIVAS UNIVERSITY uses information derived from cookies strictly for tracking usage and developing site improvements.

Outside Links

This site contains links to sites outside www.srinivasuniversity.edu.in and other sites may provide links tothis site. SRINIVAS UNIVERSITY is not responsible for the privacy practices, or the content, of such other websites. These links are provided for user convenience only. SRINIVAS UNIVERSITY does not control these other sites and assumes no liability or responsibility for them, including any content or services provided to users by such sites. Users should not consider any link to or from another site as an endorsement of that site by SRINIVAS UNIVERSITY unless SRINIVAS UNIVERSITY expressly statesso.

Personal Information

Users agree that SRINIVAS UNIVERSITY may share certain information about the user. Users agree that should the user elect to supply it, SRINIVAS UNIVERSITY may use the user name, email address, physical address, telephone, or other data to communicate with the user either by itself or through any of its designates. Users may request to have this information modified or deleted from our records. SRINIVAS UNIVERSITY may use this information as necessary to enforce these "Terms". SRINIVAS UNIVERSITY will not sell this information to any other party. These "Terms" are severable to the extent any term is deemed invalid, illegal, or unenforceable. SRINIVAS UNIVERSITY's failure to enforce any provision of these "Terms" shall not be deemed a waiver of that or any other provision of these "Terms". Users' use and continued use of the SRINIVAS UNIVERSITY's Site reflects user agreement to these "Terms" and any modifications of these "Terms" made by SRINIVAS UNIVERSITY.

Submitting Personal Information

Users can submit information to www.srinivasuniversity.edu.in in several places on the website. A'Contact Us form allows customers to request information. The form requests visitors' contact information such as their email address and/or mailing address. Contact information from the feedback form is used to send responses or information requested by our users. This information is never shared; it is used only for our replies.

Site Security

This site has security measures in place to protect the loss, misuse, and alteration of the information under our control.

A. Permission

1. SRINIVAS UNIVERSITY gives the user limited personal permission to use the website. User permission to use the website is limited in several ways. For example, users may only download or print the material contained on this Site for non-profit purposes. Any commercial use, such as selling content, creating course packs, or posting informationon another website is prohibited.
2. User may not:

- Frame all or part of the website.
- Change or delete any proprietary notices from materials downloaded or printed out from the website.
- Systemically download or print materials from the website.
- Transmit or provide any data from the website to a third party.
- Use the website in a manner contrary to any applicable law. User permission terminates immediately, without any further action by SRINIVAS UNIVERSITY, if the user breaches these "Terms".
- Users may not transfer or assign user permission to any other party.
- SRINIVAS UNIVERSITY is the owner or licensee of all rights to the website, its content, software, and services. Users have no right to such content, software, or services if not expressly granted in this agreement.
- "SRINIVAS UNIVERSITY" and the logos or other proprietary marks of SRINIVAS UNIVERSITY's licensors and partners are trademarks of SRINIVAS UNIVERSITY or its licensors and partners. No right, title, or interest in those trademarks is granted to users in this agreement.
- The site is provided "As Is ".
- Services provided through and information contained on the site are provided as is and as available. SRINIVAS UNIVERSITY makes no, and hereby disclaims any, warranty of any kind, express or implied, including but not limited to the implied warranties of title, non-infringement, merchantability, and fitness for a particular use or purpose. Further, SRINIVAS UNIVERSITY disclaims any warranty that the site will be available at all times or will operate without interruption or error. SRINIVAS UNIVERSITY makes no warranty as to the reliability, accuracy, timeliness, usefulness, adequacy, completeness, or suitability of the services or information provided through the site.
- Users alone are responsible for use of the site.
- Users agree to be solely responsible for use of this website.
- SRINIVAS UNIVERSITY, its officers, directors, employees, agents, and information providers shall not be liable for any damages users may suffer or cause through the use of the site, even if advised of the possibility of such damages.
- SRINIVAS UNIVERSITY, its officers, directors, employees, agents, and information providers shall not be liable for any direct, indirect, incidental, special, consequential, or punitive damages arising out of the use of or inability to use the site.
- These limitations shall apply whether the asserted liability or damages are based on

contract (including, but not limited to, breach of warranty), tort (including, but not limited to, negligence), or any other legal or equitable grounds.

- Users agree to indemnify and hold SRINIVAS UNIVERSITY harmless for any claims, losses, or damages, including attorney's fees, resulting from the user's breach of these terms or use of this website.

B. Children's Guidelines

Srinivas University does not knowingly collect identifiable personal information from children under age. A parent or guardian must initiate any requests for information from children under the age of 13 ontheir behalf. We encourage parents to supervise children when they browse the Internet. Privacy Protection SRINIVAS UNIVERSITY does not utilize direct mail services for "telemarketing bythe third party" so that user information will not be used for solicitation by third parties.

PROTECTION AGAINST COMPUTER VIRUSES AND MALWARE

9.1 Overview and Purpose

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents. The purpose of the Computer Virus Detection Policy is to describe the requirements for dealing with computer wireworms and Trojan horse prevention, detection, and clean-up.

9.2 Coverage

The Srinivas University Computer Virus Detection Policy applies equally to all individuals that use any Srinivas University information resources.

9.3 General Terminology

A. Email

A message, image, form, attachment, data, or other communication sent, received, or stored by an electronic mail system.

B. Incident

A recognized attempt by an unauthorized party to access a trusted network or an attack on an information system. The term encompasses unauthorized probing and browsing; Disruption or denial of service; Altered or destroyed input, processing, storage, or output of information; Loss of accountability or damage to any part of the system;, or changes to information system hardware, firmware, or software characteristics with or without users' knowledge, instruction, or intent. Incidents are generally perceived as malicious attempts to violate or degrade the confidentiality, integrity, and/or availability of informationresources.

C. Server

1. A computer program that provides services to other computer programs on the same or anothercomputer
2. A computing machine that runs a server program

D. Trojan

A destructive program—usually a virus or worm—is hidden in another piece of software, such as a game or graphics program. Trojans are typically distributed with malicious intent for harvesting data, disruptingcomputing activities, or enabling unauthorized access to restricted networks or devices.

E. Virus

A program that is attached to or embedded in an executable file or vulnerable application. Viruses deliverpayloads that can range from annoying to extremely destructive. There are many types of viruses. A file virus, for example, executes when an infected file is accessed. A macro virus infects

SRINIVAS UNIVERSITY
SRINIVAS NAGAR
MUKKA
SURATHKAL
574 146
MANGALORE

the executable code embedded in Microsoft Office programs that allow users to generate macros.

F. Worm

A software program that, once downloaded to a computer system, copies itself elsewhere on the system. Today the term is usually used to describe software that maliciously propagates itself over a network, often with the intent of overloading network capabilities. The worm is often used synonymously with "virus" however.

9.4 Policy

1. All workstations whether connected to the Srinivas University network, or standalone, must use the Srinivas University-approved virus protection software and configuration.
2. The virus protection software must not be disabled or bypassed.
3. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
4. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
5. Each file server attached to the Srinivas University network must utilize Srinivas University-approved virus protection software and set up to detect and clean viruses that may infect file shares.
6. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the point of contact or supervisor or System Administrator for further actions.

9.5 Enforcement

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; A termination of employment relations in the case of contractors or consultants; Dismissal for interns and volunteers; Or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Srinivas University information resources access privileges and civil, and criminal prosecution.

10. DATA BACKUP, STORAGE, AND RECOVERY

10.1 Overview and Purpose

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors. The purpose of this Data Backup and Storage Policy is to establish the rules for the backup and storage of Srinivas University electronic information.

10.2 Coverage

This Data Backup and Storage Policy applies to all individuals within the Srinivas University who are responsible for the installation and support of information resources, individuals charged with information resources security;, and data owners.

10.3 Services

Information services may have existing contracts for offsite backup data storage. These services can be extended to all entities of Srinivas University upon request.

10.4 Policy

1 The frequency and extent of backups must be by the importance of the information and the acceptable risk as determined by the data owner.

2 The Srinivas University Information Resources backup and recovery process for each system must be documented and periodically reviewed.

3 Any vendor(s) providing off-site backup storage for Srinivas University must be cleared to handle the highest levelof information stored.

4 Physical access controls implemented at off-site backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected

by the highest sensitivity level of information stored.

5 A process must be implemented to verify the success of the Srinivas University electronic informationbackup.

6 Backups must be periodically tested to ensure that they are recoverable.

7 Signature cards held by the offsite backup storage vendor(s) for access to Srinivas University backup media must be reviewed annually or when an authorized individual leaves Srinivas University.

8 Procedures between Srinivas University and the offsite backup storage vendor(s) must be reviewed at least annually.

9 Backup media must have at a minimum the following identifying criteria that can be readily identified by labels and/or a barcoding system:

a) System name
b) Creation date
c) Sensitivity classification [Based on applicable electronic record retention regulations]
d) Srinivas University contact information
e) Guidelines for standalone systems

A. Data backup Standards:

1. Critical data, which is critical to the university, must be defined by the university in consultation with ICT and must be backed up. Backup data must be stored at a backup location/Cloud storage that is physically different from its original creation and usage location (i.e. The Disaster Recovery Site).
2. Data backed up must at least be tested quarterly.
3. Procedures for backing up critical data and the testing of the procedures must be documented by the ITdepartment.

These procedures must include, as a minimum, for each type of data and system:

a) A definition of the specific data to be backed up
b) The type(s) of backup to be used (e.g. full back up, incremental backup, etc.)
c) The frequency and time of data backup
d) The number of generations of backed-up data that are to be maintained (both onsite and offsite)
e) Responsibility for data backup
f) The storage site(s) for the backups
g) The storage media to be used
h) Any requirements concerning the data backup archives
i) Transport modes and Recovery procedure of backed-up data.

B. Data Backup Selection and Procedures

a) All data and software essential to the continued operation of the university, as well as all data that must be maintained for legal purposes, must be backed up. All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.
b) Full backup and Incremental backup schedule should be fixed with the consultation of the IT department.
c) The schedule of the backup should be defined by the IT department.
d) The IT Department should determine the number of previous versions of operating systems and applications that must be retained at the Backup and Disaster Recovery location.
e) Data backup may be done to cloud storage and a local computer.
f) As a university has a hospital under its management, Data should be retained in line with current legislative requirements. Monthly backups must be saved for one year. Yearly backups must be retained for five consecutive financial years.
g) Recovery of Backup data: Documentation of the restoration process must include:

- Procedures for the recovery

SRINIVAS UNIVERSITY
SRINIVAS NAGAR
MUKKA
SURATHKAL
574 146
MANGALORE

- Provision for key management should the data be encrypted.

Recovery procedures must be tested at least quarterly and Disaster Recovery procedures must betested at least yearly. Recovery tests must be documented.

Disaster Recovery

For most important and time-critical data, a mirror system, or at least a mirror disk may be needed fora quick recovery. The University will plan and establish such a system.

Enforcement

Violation of this policy may result in disciplinary action, including but not limited to performance penalties, employment termination, contract invalidation, civil action, and criminal prosecution. Additionally, violators may lose access privileges to Srinivas University information resources.

11. GREEN COMPUTING

11.1 Overview and Purpose

Computers and other office machinery consume power and generate heat whenever they are on. employees should seek to optimize the power consumption of office machinery to reduce the waste, environmental impact, and energy costs associated with its use. Even small changes to the way we typically use and manage common devices can significantly reduce the amount of energy consumed by office machines. To help reduce Srinivas University's carbon footprint, save costs related to energy consumption, and extend the life of computers and other equipment, Srinivas University requires employees to follow energy-efficient computing strategies for the devices for which they have direct responsibility. Moreover, we encourage employees to apply the same principles of energy conservation to shared use devices within office environments. This policy defines steps that employees should take to conserve the energy used by computers and shared-use equipment.

11.2 Coverage

All employees, contractors, vendors, volunteers, and other personnel who use, manage or are responsible for the approval or procurement of computers and shared use equipment, including servers, network devices, office printers, copy machines, and fax machines.

11.3 Policy

A. Desktop (Personal) Computer Usage and Management

The configuration of desktop and laptop machines should be standardized so that power saving and/or energy management settings support energy-efficient operation.

Computers should be configured to enact "sleep" or "hibernation" mode whenever the computer is not in use for more than one hour, or the minimum amount of time that does not impede typical work performance.

Turn off your computer monitor when it is not in use, such as during breaks, meetings, and other periods when you are away from your computer for more than half an hour.

Turn off peripherals, such as printers, PDA devices, fax machines, and scanners, when they will not be in use for more than three hours. Check with the IT department to see if specific peripherals have "power saver" or "sleep" modes and configure devices to activate these modes at a minimal time that does not impede work performance.

If your desktop computer does not run processes overnight and is not scheduled for nightly backup, turn itoff when you leave for the day. Plug computers and other equipment into power strips instead of wall outlets, which allows the equipment to be more easily turned off.

B. Shared Use Office Device Management

i. Use the "print preview" function for office applications to review documents before printingdocuments to public printers.

ii. Avoid printing email messages and other electronic documents unless you have a specific need toretain or distribute a hard copy.

iii. If printers allow two-sided printing, use this option whenever possible.

iv. Use email or other electronic communication media whenever practical as an alternative to papermemos and faxes Copiers, faxes, and shared use office devices should be turned on only when needed.

v. Dialysis's, the first person who requires the use of a device should turn it on. Employees should turn off shared use devices at the end of each work day or, daily, at whatever time it becomes unlikely that the equipment will be used again before the next day.

C. Development, Architecture, and Infrastructure Management

IT, project, and development managers should factor energy efficiency and utility cost savings into technology decisions. Visualization technologies that optimize server use, for example, can improve the operating efficiency of server and data center environments. Development managers should consider the need for information availability in server allocation and selection. When possible, resources or processesthat may be made periodically unavailable (e.g., overnight, on weekends, and over holidays) should be housed on servers that can be periodically shut down to reduce energy consumption.

D. Data Centre Management

i. The Systems Administrator must review and document data center equipment used at least once everytwo months for:

- ➢ Excess numbers of data copies indicate inefficient use of server resources and dormancy ofinformation resources stored in the data center.
- ➢ Data that has not been accessed at least once in the previous year should be marked for removalto offline storage media.
- ➢ Servers that do not support 24×7 operations and may be turned off after work hours, over weekends,and during holidays without interfering with normal business functions.

ii. In general, office and procurement managers should review equipment requests for energy-efficient characteristics and seek energy efficient and/or green computing options for new purchases.

iii. Procurement should prefer equipment that is certified by the US Environmental Protection Agency's (EPA) "ENERGY STAR" program at a Plus 80 rating or higher.

iv. Where the cost difference between a technology alternative rated at Plus 80 is less than 10 percent higher than an alternative rated at a lower energy efficiency (all other factors being equivalent), the more efficient alternative should be purchased.

v. Laptop computers should be preferred over full-sized desktop machines. This preference may be mitigated by factors of business use, user productivity, and organizational security policy.

vi. Flat panel liquid crystal display (LCD) monitors should be preferred over conventional cathode ray tube (CRT) monitors.

vii. Printers that can print on both sides of the paper (duplex printing) should be preferred over single- side printers.

viii. Except in cases of a specific business or security need for the procurement of a dedicated printer assigned to a single individual, departmental management and procurement should encourage the use of networked/shared printers.

ix. When procurement of a personal/dedicated printer is indicated, procurement should prefer more energy-efficient inkjet printers over laser printers.

x. Procurement should actively seek and evaluate energy efficient and "green computing" offerings, noting computer vendors that offer resource-efficient machines designed for eventual recycling.

E. Equipment Reclamation, Recycling, and Disposal Management

i. Employees who are not in charge of equipment disposal should not throw away computers or other equipment, even if they are non-functional. Employees should contact the store's department to properly dispose of unused or unusable equipment.

ii. Employees who are responsible for equipment disposition should seek, whenever possible and always in compliance with secure disposal policies, to recycle, reallocate, or reuse reclaimed equipment.

iii. In cases where the entirety of a machine cannot be reused, the store's department should seek to salvage and reuse any valuable components.

iv. CRT monitors contain hazardous materials and must be disposed of in compliance with the Government of India's Environment Policies Enforcement.

v. Willful violation of this policy may result in disciplinary action which may include performance sanctions; Termination for employees and temporaries; A termination of employment relations in the case of contractors or consultants; Dismissal for interns and volunteers; Or suspension or expulsion in the case of a student.

vi. Additionally, individuals are subject to restriction or suspension of the Srinivas University email privileges, as well as civil and criminal prosecution.

SRINIVAS UNIVERSITY
SRINIVAS NAGAR
MUKKA
SURATHKAL
574 146
MANGALORE

VIDEO SURVEILLANCE POLICY

12. The Systems

i. The system comprises fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; Digital recorders; SAN/NAS Storage; Public information signs.

ii. Cameras will be located at strategic points on the campus, principally at the entrance and exit points of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontage or rear areas of private accommodation.

iii. Signs will be prominently placed at strategic points and at the entrance and exit points of the campus to inform staff, students, visitors, and members of the public that a CCTV/IP camera installation is in use.

iv. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

12.1 Purpose of the system

1. The system has been installed by Srinivas University with the primary purpose of reducing the threatof crime generally, protecting Srinivas University premises, and helping to ensure the safety of all staff, students, patients, and visitors consistent with respect for the individual's privacy.

These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension, and prosecution of offenders of crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff orstudent against whom disciplinary or other action is, or is threatened to be taken.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment

2. The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than by the policy on the covert recording.
- For any automated decision-making.

3. Covert recording

Covert cameras may be used under the following circumstances on the written authorization of the Board of Management:

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorized or illegal activity is taking place or is about to take place.

4. Any such covert processing will only be carried out for a limited and reasonable period consistent with the objectives of making the recording and will only relate to the specific suspected unauthorized activity.

5. The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

SRINIVAS UNIVERSITY
SRINIVAS NAGAR
MUKKA
SURATHKAL
574 146
MANGALORE

12.2 The Security Control Room

1. Images captured by the system will be monitored and recorded in the Security Control Rooms, "the control rooms", twenty-four hours a day throughout the whole year. Monitors are not visible from outsidethe control room.
2. No unauthorized access to the Control Rooms will be permitted at any time. Access will be strictly limited to the duty controllers/officers, authorized members of senior management, police officers, and any other person with statutory powers of entry.
3. Staff, students, and visitors may be granted access to the Control Rooms on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room.
4. Before allowing access to the Control Rooms, staff will satisfy themselves with the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization they represent, the person who granted authorization, and the times of entry to and exit from the center. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

12.3 Security Control Room Administration and Procedures:

1. Details of the administrative procedures which apply to the Control Rooms will be set out in a procedures manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.
2. Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisors are responsible for ensuring day-to-day compliance with the Act. All recordings willbe handled in strict accordance with this policy and the procedures set out in the procedures manual.

12.4 Staff

All staff working in the Security Control Rooms will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisors will ensure that all staff is fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

12.5 Recording

1. Digital recordings are made using digital video recorders operating in time-lapse mode. Incidents may be recorded in real-time.
2. Images will normally be retained for fifteen days from the date of recording, and then automatically overwritten and the Log updated accordingly. Once a hard drive has reached the end of its use it willbe erased before disposal and the log will be updated accordingly.
3. All hard drives and recorders shall remain the property of Srinivas University until disposal and destruction.

12.6 Access to images

1. All access to images will be recorded in the access log as specified in the procedures manual
2. Access to images will be restricted to those staff who need to have access to the system.
3. Access to images by third parties:

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images are recorded would assist in a criminal inquiry and/or theprevention of terrorism and disorder

- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of a crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal inquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

Access to images by a subject:

CCTV/IP camera digital images, if they show a recognizable person, are personal data and are covered bythe Data Protection Act. Anyone who believes that they have been filmed by C.C.T.V. /IP camera is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right to instant access.

a. A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. Subject Access Request Forms are obtainable from the Security Office, between the hours of 9 AM to 01 PM Monday to Saturday, except when Srinivas University is officially closed, or from the Data Protection Officer, the Records Office during the same hours.

b. The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyoneelse for a copy of the data. All communications must go through the Srinivas University Data Protection Officer. A response will be provided promptly and in any event within forty days of receiving the requiredfee and information.

c. The Data Protection Act gives the Data Protection Officer the right to refuse a request for a copy of the data, particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

d. All such requests will be referred to the Security Control Room Supervisors or by the Data ProtectionOfficer.

e. If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

12.7 Request to prevent processing

1. An individual has the right to request the prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.
2. All such requests should be addressed in the first instance to the respective Security Control Room Supervisor or the Data Protection Officer, who will provide a written response within 21 days ofreceiving the request and setting out their decision on the request. A copy of the request and response willbe retained.

12.8 Complaints

It is recognized that members of Srinivas University and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security ControlRoom supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Srinivas University Centralized Complaints Procedure by obtaining and completing a Srinivas University Complaints Form and a copy of the procedure. Complaints forms maybe obtained from the Systems Administrator. Concerns or inquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer, these rights do not alter the existing rights of members of Srinivas University or others under any relevant grievance or disciplinary procedures.

12.9 Compliance monitoring

1. The contact point for members of Srinivas University or members of the public wishing to enquire about the system will be the Security Office which will be available during the working hours from

Monday to Saturday except when Srinivas University is officially closed.

2. Upon request enquirers will be provided with: A summary of this statement of policyAn access request form if required or requested
3. A subject access request form if required or requested Copy of the Srinivas University CentralComplaints Procedures
4. The documented procedures will be kept under review and a report periodically be made to theBoard of Management through the Registrar-Srinivas University.
5. The effectiveness of the system in meeting its purposes will be kept under review and reportssubmitted as required to the Board of Management through Registrar- Srinivas University.

SRINIVAS UNIVERSITY
SRINIVAS NAGAR
MUKKA
SURATHKAL
574 146
MANGALORE

13. APPENDIX

13.1 Appendix- I

Campus Network Services Use Agreement

Read the following important policies before applying for the user account/email account. By signing the application form for IP address allocation Access ID (user account)/email account, you agree to act bythe IT policies and guidelines of Srinivas University. Failure to comply with these policies may result in the termination of your account/IP address. It is only a summary of the important IT policies of SrinivasUniversity User can have a copy of the detailed document from the Intranet (viz. **http://Srinivas University.edu.in**).

A Net Access ID is the combination of a user name and a password whereby you gain access to Srinivas University computer systems, services, campus networks, and the internet.

1. **Accounts and Passwords**

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. The User will not share the password or Net Access ID with anyone. Network IDs will only be established for students, staff, and faculty who are currently affiliated with Srinivas University. Students, staff, and faculty who leave Srinivas University will have their Net Access ID and associated files deleted (After approval from HR Section and IT department). No User will be allowed more than one Net Access ID at a time, with the exception that faculty or officers who hold more than one portfolio, are entitled to have a Net Access ID related to the functions of that portfolio.

2. **Limitations on the use of resources**

On behalf of Srinivas University, the IT department reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

3. **Computer Ethics and Etiquette**

The User will not attempt to override or break the security of the Srinivas University computers, networks, or machines/networks accessible there. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing abusive, obscene, or fraudulent messages. Even sending unsolicited bulk e-mail messages comes under IT policy violation. In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used. User's net access ID gives him/her access to e-mail, and campus computing resources. The use of these resources must comply with Srinivas University policy and applicable. Electronically available information.

a) may not contain copyrighted material or software unless permission of the copyright owner has beenobtained,
b) may not violate Srinivas University policy prohibiting sexual harassment,
c) may not be used for commercial purposes,
d) should not appear to represent the Srinivas University without appropriate permission, or to representothers,
e) may not appear to represent other organizations or companies,
f) may not contain material that violates pornography laws, or algorithms or software which if transferred violate laws,
g) may not contain scripts or code that could cause a security breach or permit use of resources inopposition to Srinivas University policy, and

WWW pages should clearly show identifying information of the owner of the page and we suggest that it also show the date of last revision and an address (e-mail or postal) for correspondence. IT

h) Department equipment does not support the use of scripting on individual pages.

4. **Data Backup, Security, and Disclaimer**

IT department will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an IT department staff member in the process ofhelping the user in resolving their network/computer related problems. Although IT Department makes a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibilityfor backing up files in the assigned Net Access ID, storage space, or email Account. In addition, the IT department makes no guarantee concerning the security or privacy of a user's electronic messages.

The user agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold the IT department as part of Srinivas University, harmless for any such liability or expenses. Srinivas University retains the right to change and update these policies as required without notification to the user.

5. **Account Termination and Appeal Process:**

Accounts on Srinivas University network systems may be terminated or disabled with little or no notice for any of the reasons stated above or for other inappropriate use of computing and network resources. When an account is terminated or disabled, the IT department will make an attempt to contact the user (at the phone number they have on file with the IT department) and notify them of the action and the reason for the action. If the termination of an account is temporary, due to inadvertent reasons and on the grounds of virus infection, the account will be restored as soon as the user approaches and takes the necessary steps to get the problem rectified and communicates to the IT department of the same, but, if the termination of account is on the grounds of wilful breach of IT policies of the Srinivas University by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may first approach the Head of the IT department, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Registrar/ appeal board duly constituted by the Srinivas University for this purpose to review the evidence and hear reasons why an appeal should be considered. If the Appeals Board recommends the revival of the account, it will be enabled. However, the Decision of the Appeals Board is final and should not be contested. users may note that the Srinivas University Network Security System maintains ahistory of infractions, if any, for each user account. In case of any termination of a user account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before Vice Chancellor for furtheactionns.

Policy Supporting **Documentation**Service and Conduct Rules Srinivas	**Policy Support** **Contact**Systems Administrator