SHIVAJI UNIVERSITY, KOLHAPUR.

IT Policy & Guidelines

(Release: Jan. 2014 Version 1.0)

(Revised on Oct. 2019 Version 2.0)

Prepared by
Computer Center,
Shivaji University,
Vidya Nagar, Kolhapur 416004.

Shivaji University's IT Policy

(Release: Jan. 2014 Version 1.0)

(Revised on Oct 2019 Version 2.0)

Need for IT Policy

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

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions & research organizations. Realizing the importance of these services, SUK took initiative way back in 2000 and established basic network infrastructure in the academic complex of the university.

Over the last ten years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the university's academic environment. Considering this change Shivaji University decided to upgrade the network Infrastructure again in 2012.

Now, the university has about 3500 network connections covering more than ~~twenty~~ buildings across the campus and expected to reach 4000 connections very soon.

Internet Unit of Computer Center is the department that has been given the responsibility of running the university's intranet & Internet services.

Internet Unit is running the Firewall security, Proxy, DHCP, DNS, email, web and application servers and managing the network of the university.

SUK is getting its Internet bandwidth from BSNL. Total bandwidth availability from BSNL source is 225(100+100+25) Mbps (leased line). SUK has also got 1 Gbps connectivity under NKN Network of MHRD (NME-ICT) via BSNL.

While educational institutions are providing access to Internet to their faculty, students and staff, they face certain constraints:

- Limited Internet bandwidth.
- Limited infrastructure like computers, computer laboratories,
- Limited financial resources in which faculty, students and staff should be provided with the network facilities and
- Limited technical manpower needed for network management.

On one hand, resources are not easily available for expansion to accommodate the continuous rise in Internet needs, on the other hand uncontrolled, uninterrupted and free web access can give rise to activities that are neither related to Teaching/learning processes nor governance of the university.

At the outset, we need to recognize the problems related to uncontrolled surfing by the users:

- Prolonged or intermittent surfing, affecting quality of work
- Heavy downloads that lead to choking of available bandwidth
- Exposure to legal liability and cases of sexual harassment due to harmful and embarrassing content.
- Confidential information being made public.

.

With the extensive use of the Internet, network performance suffers in three ways:

When compared to the speed of Local Area Network (LAN), Internet traffic over the Wide Area Network (WAN) is a potential bottleneck.

When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.

 When computer systems are networked, viruses that get into the LAN, through Intranet/Internet, spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

Too many concurrent users who are on the high speed LANs trying to access Internet resources through a limited bandwidth, definitely create stress on the Internet bandwidth available.

Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down the Quality of Service. Reducing Internet traffic is the answer.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. Others simply attach themselves to files and replicate themselves, taking up network space and slowing down the network.

Apart from this, plenty of employee time is lost with a workstation being scanned and cleaned of the virus. Emails, unsafe downloads, file sharing and web surfing account for most of the virus attacks on networks. Once they gain entry into the network, viruses attach themselves to files, replicate quickly and cause untold damage to information on the network. They can slow down or even bring the network to a halt. Containing a virus once it spreads through the network is not an easy job. Plenty of man-hours and possibly data are lost in making the network safe once more. So preventing it at the earliest is crucial.

Hence, in order to securing the network, Computer Center has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway. However, in the absence of clearly defined IT policies, it is extremely 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. As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions.

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.
An effective security policy is necessary to a good information security program as a solid foundation to the building.
Hence, Shivaji University also is proposing to have its own IT Policy that works as guidelines for using the university's computing facilities including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called "Information Technology (IT)". Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this 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, Information security in general and therefore policies that govern information security process 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.
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 university community to understand how University policy applies to some of the significant areas and to bring conformance with stated policies.
IT policies may be classified into following groups:

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Web Site Hosting Policy
- University Database Use Policy

Further, the policies will be applicable at two levels :

- End Users Groups (Faculty, students, Senior administrators, Officers and other staff)
- Network Administrators

It may be noted that university IT Policy applies to technology administered by the university centrally or by the individual departments, to information services provided by the university administration, or by the individual departments, or by individuals of the university community, or by authorized resident or non-resident visitors on their own hardware connected to the university network. This IT policy also applies to the resources administered by the central administrative departments such as Library, Laboratories, Offices of the university recognized Associations/Unions, or hostels and guest houses, Teaching Departments or residences wherever the network facility was provided by the 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 university IT policy.

Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the University's information technology infrastructure , must comply with the Guidelines. Certain violations of IT policy laid down by the university by any university member may even result in disciplinary action against the offender by the university authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

Stake holders on campus or off campus

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

Resources

- Network Devices wired/ wireless
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Mobile/ Desktop / laptops / server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

1] IT Hardware Installation

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

A. **Who is Primary User**

An individual in whose room 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 should make an arrangement and make a person responsible for compliance.

B. **What are End User Computer Systems**

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

C. **Warranty & Annual Maintenance Contract**

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking virus related problems also.

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

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

E. **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.

F. **File and Print Sharing Facilities**

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

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

Computer system may be moved from one location to another with prior written intimation to the COMPUTER CENTER, as COMPUTER CENTER maintains the record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation (from the list maintained by COMPUTER CENTER 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 Internet Unit of Computer Center in writing/by email, connection will be restored.

H. **Maintenance of Computer Systems provided by the University**

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

I. Noncompliance

SUK 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 university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be non-compliant.

J. COMPUTER CENTER/ INTERNET UNIT Interface

INTERNET UNIT 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 COMPUTER CENTER. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT will provide guidance as needed for the individual to gain compliance. User can report his complaint to it.support@unishivaji.ac.in on this official email ID.

2] Software Installation and Licensing

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

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

A. Operating System and its Updating

1. 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.
2. University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

3. Computers under university domain controller, will get Microsoft updates automatically from university's WSUS/SEQURITE PATCH MANAGEMENT SERVER. Even if the systems are configured for automatic updates, it is users responsibility to make sure that the updates a being done properly.

B. Antivirus Software and its updating

1. Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.
2. 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 end user's technical skills, the end-user is responsible for seeking assistance from Computer Center or any service-providing agency.

C. 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 drive and 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 C drive volume, will protect the data loss. However, it is not a foolproof solution. Apart from this, users should keep their valuable data either on portable hard disk or other reliable storage devices.

3] Network (Intranet & Internet) Use

Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy. The Communication & Information Services (INTERNET UNIT) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to INTERNET UNIT on it.support@unishivaji.ac.in

A. IP Address Allocation

Any computer (PC/laptop/Server) that will be connected to the university network, should have an IP address assigned by the INTERNET UNIT. 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 unauthorized from any other location.
Any IP base device like network printer, smart TV, bio metric machine, CCTV DVR, IP Camera, Video conferencing device, IP Phone etc. is to be install at any location, then the concern user should contact Internet Unit and get proper IP Address.
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..

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

Use of any computer at end user location as a DHCP server or Wi-Fi router 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 university. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by INTERNET UNIT. Even configuration of any computer with additional network interface card or creating Wi-Fi hot spots 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 department/user.

C. Running Network Services on the Servers

Individual departments/individuals connecting to the university network over the
LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after bringing it to the knowledge of the INTERNET UNIT in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network. INTERNET UNIT takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property. INTERNET UNIT 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 University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes. Network traffic will be monitored for security and for performance reasons at University Campus. 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.

D. Wi-Fi/Cellular/Dial-up/Broadband Connections

Wi-Fi routers, mobiles, USB Broad band modem, Computer systems or any such devices that are part of the University's campus-wide network, whether university's property or personal property, should not be used for dial-up/broadband connections, as it violates the

university's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

E. Wireless Local Area Networks

1. This policy applies, in its entirety, to School, department, or division wireless local area networks. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with INTERNET UNIT including Point of Contact information.
2. School, departments, or divisions must inform INTERNET UNIT for the use of radio spectrum , prior to implementation of wireless local area networks.
3. School, departments, or divisions 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.
4. If individual School wants to have inter-building wireless network, prior to installation of such network, it should obtain permission from the university authorities whose application may be routed through the Co-ordinator, INTERNET UNIT.

F. Internet Bandwidth obtained by Other Departments

Internet bandwidth acquired by any Section, department of the university under any research program/project should ideally be pooled with the university's Internet bandwidth, and be treated as university's common resource. Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such network should be totally separated from the university's campus network. All the computer systems using that network should have separate IP address scheme (private as well as public) and the university gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the university IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to INTERNET UNIT.

G. Un-authorized Network expansion

Any user or department is not allowed to connect additional desktop network switch as it may create loops or unwanted traffic. If it is very essential, then user / department must get proper permission from Internet Unit. Non-compliance to this policy will be direct violation of the university's IT security policy.

4] Internet Access

Normally Internet access is available to all computers, laptops, servers, mobile devices and other IP based devices which are authorized to connect to the campus network.

It is responsibility of the individual to access Internet in the ethical and legitimate manner. Sometimes the user is unware of risks in accessing some websites/web applications/apps and may get infected with virus, malware, adware or expose vulnerability. Therefore, users are broadly categorized as faculty, research students, UG/PG students, officers, clerical staff and technical staff. Depending on the category Internet access will be filtered at firewall. So that intentional or unintentional access to malicious websites/web applications (eg. Gaming, streaming, social media, online shopping etc.) will be avoided by default.

In case a website is filtered out, however it is essential for academic and administrative purpose, then the individual/ section/ department may request to Internet Unit. After verifying the need, authenticity and safety, Internet Unit will make the requested website available. (eg. Banking sites, payment sites, and temporary links on Government sites etc.)

5] Wi-Fi implementation and usage

Applies to

Stake holders on campus or off campus

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

Resources

- Wi-Fi Access Points /routers installed by University
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Multimedia Contents

Wi-Fi facility is implemented for the above mentioned stake holders in the campus. For uniform and efficient and solicited usage of the WiFi facility policies are defined as follows:

Wi-Fi Access and locations

1. Wi-Fi Access Point Location: Almost all buildings in the campus have been built using stones. Therefore implementing Wi-Fi facility was a great challenge. Making Wi-Fi available in every room will not be economic. Furthermore, it was suggested that Wi-Fi facility may be made available in mostly at common places like canteen, library, hostel corridors, department corridors, Laboratories, guest house and officers residences etc.
2. Wi-Fi Access Points may not be placed in the classroom.
3. Wi-Fi Access Points may be placed temporarily on demand in auditoria and other places, for conference, workshops, symposia and any other important events.
4. Personal Wi-Fi Access devices may not be allowed; as such devices may cause disturbance in IP allotment and security threat to University's Network. If found the personal devices may be confiscated by Internet Unit.
5. In special cases the individual or department may approach to Internet Unit and get proper secure configuration and registration of the personal/ department's Access Points or routers.

Methods for Wi-Fi users Authentication/ Authorization and Activity Logs

For Wi-Fi access physical connectivity between client and Access point is not necessary. Hence, if proper care is not taken then any person with Wi-Fi enabled device may access the Wi-Fi services. Therefore, to prevent unauthorised access, identification/ authentication, authorization and activity logs of the users is a must. Following action plan is devised for one time registration/identification of the authorised devices and users:

6. Device identification by MAC (Media Access Control) and user identification by Employee number of Faculty, administrative officers and authorities. This is one time process. Data is collected from Establishment Section and Pay bills Section.
7. In case of Research Students PRN is used for their identification, which is printed on their Library card.
8. UG/PG students on the campus are given Wi-Fi Access based on their PRN and some other parameters. On one time registration the device of the student is registered for the period depending on their Course. After completion of the course duration the user will be automatically deleted from the system. On the commencement of academic year, the academic departments should provide the list of their students in prescribed format on email to Internet Unit.
9. For respected guests/invitees staying in the campus Wi-Fi access is given on demand by the corresponding hosts. It is password based access. Passwords are changed periodically by Internet Unit.

Changes/ Modifications in the user details

10. In case a mobile device is lost/stolen/sold/transferred the user should intimate the Internet Unit immediately.
11. For Wi-Fi access to new mobile device an employee should intimate the new MAC Id of the device to Internet Unit by an email sent from his/her official email id. Internet Unit will modify accordingly.

12. For Wi-Fi access to new mobile device a student should intimate the new MAC Id of the device to Internet Unit by an application forwarded through the respective Head of the Department.

Wi-Fi Usage

13. The individual user will be responsible for his/her Wi-Fi usage made.
14. Solicited and ethical usage is expected from the users.
15. The Internet Access through Wi-Fi is filtered access. Possible phishing, spurious, unsolicited or obscene sites, gaming sites, some shopping/multimedia streaming site are blocked at firewall level.
16. There shall be per day usage quota on Students User class.
17. The users will access the University Resources properly and will not try to harm the resources.

Misuse and actions

18. If a user or his/her device is making any harm to university resources or other users, then such a user will be warned by Internet Unit. User's intention and device are verified. The corresponding Head of the department will be informed accordingly.
19. A virus infected device may create noticeable network traffic or attempts cyber-attacks. Then the user will be notified and his/her access shall be blocked until the infected device is cleaned/ free from viral infection.

6] Email Account Use

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc. To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to **http://mail.unishivaji.ac.in** with their User **ID** and **password**. For obtaining the university's email account, user may contact INTERNET UNIT for email account and default password by submitting an application in a prescribed format. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. the facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

3. while sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks 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.
6. Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.
7. 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.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
10. Impersonating email account of others will be taken as a serious offence under the university IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.
12. Any Spam mail received by the user into INBOX should be forwarded to spam@mail.unishivaji.ac.in
13. Any mail wrongly stamped as SPAM mail should be forwarded to wrongspam@mail.unishivaji.ac.in
14. All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. If so, user may forward that mail ID to netadmin@unishivaji.ac.in for necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.

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

7] Web Site Hosting

1. Official Pages

Sections, departments, and Associations of Teachers/Employees/Students may have pages on SUK's Intranet Channel of the official Web page. Official Web pages must conform to the University Web Site Creation Guidelines for Web site hosting. As on date, the university's webmaster is responsible for maintaining the official web site of the university viz., http://www.unishivaji.ac.in only.

2. Personal Pages:

The university computer and network infrastructure is a limited resource owned by the university. It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the university by sending a written request to INTERNET UNIT giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the university. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups.

Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the university.

3. Affiliated Pages:

Faculty may host Web pages for "affiliated" professional organizations on department Web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

4. Web Pages for eLearning

Faculty 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 University's Web for eLearning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official SUK or other Web sites. If a student publishes a fictional Web site or a Web site modeled 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:

5. 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 eLearning purpose.

6. Maintenance:

If the pages are published on the eLearning information server, they will be maintained under the default rules for personal eLearning pages

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

7. **Content Disclaimer:**

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

8. **Policies for Maintaining Web Pages**

Pages must relate to the University's mission. Authors of official SUK and affiliated pages are required to announce their Web presence by sending an announcement to webmaster@unishivaji.ac.in. Mails sent to this address will be placed in a SUK Public E-Mail Folder in the SUK's official web site.. The announcement should include:

1. The URL.
2. A brief explanation of content or purpose of the pages (i.e., Web pages for an administrative or academic unit, etc.). The primary page must include a link to the SUK Home Page and, if applicable, contain additional links to the sponsoring organization or department.

8] Network Protocol Access

As a standard practice HTTP, HTTPS, FTP, SMTP, DNS are the protocols available to all users in the campus. In case a genuine website is hosted on some other protocol or port, then the user/ section / department may inform the Internet Unit. After verifying the need, authenticity and safety, Internet Unit will make the requested website and protocol available.

For academic or administrative work some web applications hosted on the University servers. Such web applications should be hosted on standard HTTP and/or HTTPS ports only. Virtual Web Directory Method may be used to host multiple web applications on standard ports.

9] University Database (of e-Governance) Use

This Policy relates to the databases maintained by the university administration under the university's e-Governance.

Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential.

SUK has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the university's approach to both the access and use of this university resource.

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

B. **Custodians of Data:** Individual Sections or departments generate portions of data that constitute University's database. They may have custodianship responsibilities for portions of that data.

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

D. **MIS Components:** For the purpose of e-Governance, Management Information System requirements of the university may broadly be divided into seven categories. These are:

- MANPOWER INFORMATION MANAGEMENT SYSTEM (MIMS)
- STUDENTS INFORMATION MANAGEMENT SYSTEM (SIMS)
- FINANCIAL INFORMATION MANAGEMENT SYSTEM (FIMS)
- PHYSICAL RESOURCES INFORMATION MANAGEMENT SYSTEM (PRIMS)
- PROJECT INFORMATION MONITORING SYSTEM (PIMS)
- LIBRARY INFORMATION MANAGEMENT SYSTEM (LIMS)
- DOCUMENT MANAGEMENT AND INFORMATION RETRIEVAL SYSTEM (DMIRS)

Here are some general policy guidelines and parameters for Sections, departments and administrative unit data users:

1. The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.
2. Data from the University's Database including data collected by departments or individual faculty and staff, is for internal university purposes only.
3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies the university makes information and data available based on those responsibilities/rights.
4. Data directly identifying a person and his/her 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 University Registrar.
5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the University and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the University Registrar for response.
6. 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 university or its departments.
7. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar, Director, Board of Examination and Evaluation and Finance and Accounts officer of the University.
8. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.
9. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to :
    - Modifying/deleting the data items or software components by using illegal access methods.
    - Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
    - Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.

- Trying to break security of the Database servers.

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

10] Video Surveillance

The system

10.1.1 The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.

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

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

10.1.4 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.

10.2.0 Purpose of the system

10.2.1 The system has been installed by university with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' 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 in relation to 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 or student 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

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

10.2.2 Covert recording

Covert cameras may be used under the following circumstances on the written authorization or request of the Senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer

- 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.

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

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.

10.3.0 The Security Control Room

10.3.1 Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

10.3.2 No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, police officers and any other person with statutory powers of entry..

10.3.3 Staff, students and visitors may be granted access to the Control Room 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.

10.3.4 Before allowing access to the Control Room, staff will satisfy themselves of 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.

10.4.0 Security Control Room Administration and Procedures

10.4.1 Details of the administrative procedures which apply to the Control Room 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.

10.4.2 Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

10.5.0 Staff

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

10.6.0 Recording

10.6.1 Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

10.6.2 Images will normally be retained for **fifteen** days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

10.6.3 All hard drives and recorders shall remain the property of university until disposal and destruction.

10.7.0 Access to images

10.7.1 All access to images will be recorded in the Access Log as specified in the Procedures Manual

10.7.2 Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

10.7.3 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 recorded would assist in a criminal enquiry and/or the prevention 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 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 enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

10.7.4 Access to images by a subject

CCTV/IP Camera digital images, if they show a recognisable person, are personal data and are covered by the 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 of instant access.

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 1020 and 1400 and 1430 to 1800 Monday to Saturday (except Second and fourth Saturday), except when university is officially closed or from the Data Protection Officer, the Records Office during the same hours.

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 anyone else for a copy of the data. All communications must go through the university Data Protection Officer. A response will be provided promptly and in any event within forty days of receiving the required fee and information.

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.

All such requests will be referred to the Security Control room Supervisor or by the Data Protection Officer.

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.

10.8.0 Request to prevent processing

10.8.1 An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

10.8.2 All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Data Protection Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

10.9.0 Complaints

10.9.1 It is recognised that members of 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 Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralised Complaints Procedure by obtaining and completing a University Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries 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 University or others under any relevant grievance or disciplinary procedures.

10.10 Compliance monitoring

10.10.1 The contact point for members of University or members of the public wishing to enquire about the system will be the Security Office which will be available during the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday (except second and fourth Saturday) except when University is officially closed.

10.10.2 Upon request enquirers will be provided with:

A summary of this statement of policy

An access request form if required or requested

A subject access request form if required or requested

A copy of the University central complaints procedures

10.10.3 All documented procedures will be kept under review and a report periodically made to the Estates Management Committee.

10. 10.4 The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to the Estates Management Committee.

11. Purchase

Summary

The policy is to establish the procedure for the purchase of computer hardware, software, networking equipment and allied material.

Policy:

The purchase of computer hardware, software, networking equipment and allied material shall be done after the approval from the Board of Information Technology as applicable clause under Maharashtra University Act 2016, Section 50(n). The purchase procedure shall be as per the university 'Account Code'.

Acceptable Usage Policy (SUK: Shivaji University, Kolhapur)

Computer Usage: The purpose of University (SUK) policies regarding computer and network usage is to protect all individuals affiliated with University. Inappropriate use exposes the University to risks, including virus attacks, compromise of network systems and services, and possible legal liability. Access to the information technology environment at University is a privilege and must be treated as such by all users. Students are expected to be positive members of the University community, which extends to cyberspace, by following the Community Code and all University policies. Users who violate any acceptable use policy will be subject to disciplinary action, up to and including loss of privileges and/or expulsion, and may be at risk for civil or criminal prosecution. All violations will be handled in accordance with University policies and procedures.

Following is a brief summary of relevant University policies regarding computer and network usage. All policies in their entirety can be found on the University's website or requested from the University Computer Center **(CC)** Office.

Acceptable Use Policy: University information technology resources, including electronic communications on and off the campus and the computers attached to this network, are for the use of persons currently affiliated with University, including faculty, staff and students. Information technology resources are provided by the University to further the mission of e-governance and lifelong education. Use of these resources should be consistent with this mission and this policy. Central to appropriate and responsible use is

the stipulation that computing resources shall be used in a manner consistent with the instructional, public service, research, and administrative objectives of the University. Use should also be consistent with the specific objectives of the project or task for which such use was authorized. All uses inconsistent with these objectives are considered to be inappropriate use and may jeopardize further access to services.

This Acceptable Usage Policy covers the security and use of all (SUK's) information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all (SUK's) employees, Students, Guests, Temporary Employee's, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to (SUK's) academic and administrative activities worldwide, and to all information handled by (SUK) relating to other organization's with whom it deals. It also covers all IT and information communications facilities operated by (SUK) or on its behalf.

Unacceptable uses include, but are not limited to, the following:

- Using the resources for any purpose that violates University/State Act.

- Using the resources for commercial purposes, sales and/or advertising.

- Using excessive data storage or network bandwidth in such activities as propagating of

  "chain letters" or "broadcasting" inappropriate messages to lists or individuals or generally transferring unusually large or numerous files or messages.

- Sending or storing for retrieval patently harassing, intimidating, or abusive material.

- Misrepresenting your identity or affiliation in the use of information technology resources.

- Using someone else's identity and password for access to information technology resources or using the network to make unauthorized entry to other computational, information or communications devices or resources.

- Attempting to evade, disable or “crack” password or other security provisions of systems on the network.

- Reproducing and/or distributing copyrighted materials without appropriate authorization.

- Copying or modifying files belonging to others or to the University without authorization including altering data, introducing or propagating viruses or worms, or simply damaging files.

- Interfering with or disrupting another information technology user’s work as well as the proper function of information processing and network services or equipment.

- Intercepting or altering network packets.

Computer Access Control – Individual’s Responsibility

Access to the (SUK) IT systems is controlled by the use of User IDs, passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the (SUK’s) IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any (SUK) IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else’s user ID and password to access (SUK’s) IT systems. Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to (SUK’s) IT systems or information. Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific Academic and Administrative need to interrogate the system or data.
- Connect any non-(SUK) authorised device to the (SUK) network or IT systems.
- Store (SUK) data on any non-authorised (SUK) equipment. Give or transfer (SUK) data or software to any person or organisation. Outside (SUK) without prior permission from (SUK) authorities.

Internet and email Conditions of Use

Use of (SUK) internet and email is intended for Academic and Administrative use. Personal use is permitted where such use does not affect the individual's Academic and Administrative performance, is not detrimental to (SUK) in any way, not in breach of any term and condition of employment and does not place the individual or (SUK) in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which (SUK) considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal Academic and Administrative.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to (SUK), alter any information about it, or express any opinion about (SUK), unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward (SUK) mail to personal (non-SUK) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of (SUK) unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect (SUK) devices to the internet using non-standard connections. Like external USB Modem, Mobile Devices, Jio Wi-Fi etc.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, (SUK) enforces a clear desk and screen policy as follows:

- Personal or confidential Academic and Administrative information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All Academic and Administrative-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with (SUK) remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only (SUK) authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must use only software that is authorised by (SUK) on (SUK's) computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on (SUK) computers must be approved and installed by the (SUK) IT department.

Individuals must not:

- Store personal files such as music, video, photographs or games on (SUK) IT equipment. i.e. Servers and Storage Equipment's

Viruses

The IT department has implemented centralized, automated virus detection and virus software updates within the (SUK). All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved (SUK) anti-virus software and procedures.
- Install Anti-virus solution from any other brand/product (unauthorised / not licensing)

Telephony (Voice) Equipment Conditions of Use

Use of (SUK) voice equipment is intended for Academic and Administrative use. Individuals must not use (SUK's) voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

- Use (SUK's) voice for conducting private Academic and Administrative. Make hoax or threatening calls to Internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for Academic and Administrative use.

Actions upon Termination of Contract/Course completion/Service

- All (SUK) equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to (SUK) at termination of contract**/**Course completion/Service.
- All (SUK) data or intellectual property developed or gained during the period of employment remains the property of (SUK) and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

- All data that is created and stored on (SUK) computers is the property of (SUK) and there is no official provision for individual data privacy, however wherever possible (SUK) will avoid opening personal emails.
- IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. (SUK) has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.
- Any monitoring will be carried out in accordance with audited, controlled internal processes, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Academic and Administrative Practice Interception of Communications) Regulations 2000.

  This policy must be read in conjunction with:

- Information Technology (IT) Policy 2014 of SUK's and its amendment's
- Information Technology (IT) Law 2000 and its amendment's

It is individual responsibility to report suspected breaches of security policy without delay to computer center and Internet Unit through proper channel.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with (SUK) disciplinary procedures.

I have read the User Acceptance policy above and will adhere to the guidance outlined in accordance with the policy.

Signed:…… **name:……**

Date:……..

Guidelines on Computer Naming Conventions

1. In order to troubleshoot network problems and provide timely service, it is vital to be able to quickly identify computers that are on the campus network. All computer names on the campus network must use the University standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of INTERNET UNIT.
2. All the computers should follow the standard naming convention as follows
3. The desktops on the campus are Named as
   e.g PHYD001 Where PHY is Department/Section Abbreviation, D- Desktop, 001 – Sequence number.
4. The Laptops on the campus are Named as
   e.g CHEML001 Where CHEM is Department/Section Abbreviation, L- Laptop, 001 – Sequence number.

Guidelines for running Application or Information Servers

Running Application or Information Servers

i Section/Departments may run an application or information server.

ii Individual faculty, staff or students on the SUK campus may not run personal, publicly available application or information servers (including content or services providing programs such as ftp, chat, news, games, mail, ISP, etc.) on the SUK network.

Responsibilities for Those Running Application or Information Servers

Sections/Departments may run an application or information server. They are responsible for maintaining their own servers.

1) Application or information server content and services must follow content guidelines as described in SUK Guidelines for Web Presence.

2) Obtain an IP address from INTERNET UNIT to be used on the server

3) Get the hostname of the server entered in the DNS server for IP Address resolution. University IT Policy's naming convention should be followed while giving the host names.

4) Make sure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.

5) Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam etc.

6) Operating System and the other security software should be periodically updated.

7) Sections/Departments may run an application or information server provided they do the following:

I. Provide their own computer, software and support staff

II. Provide prior information in writing to INTERNET UNIT on installing such Servers and obtain necessary IP address for this purpose.

For general information to help you decide whether or not to run a department or organization web server, contact the INTERNET UNIT.

Guidelines for hosting Web pages on the Internet/Intranet.

Mandatory:

1. Provide the full Internet e-mail address of the Web page maintainer.
2. Provide a link to the SUK home page from the parent (department of origin) home page.
3 Provide a link to the parent home page ("Return to department's home page") on all supporting local pages.
4. Maintain up to date pages. Proofread pages and test links before putting them on the Web, and regularly test and update links.
5. Know the function of HTML tags and use them appropriately.
6 Make provision for providing information without images as printer-friendly versions of the important web pages.
7. It is the responsibility of the concern department / section to keep the updated information
on their webpages. All old information has to be removed from university website.
8. Each department / Section should visit daily to check their information on website.
9. In case of any RTI filed, then concern department / section has to reply to the concern applicant .
10. It is the responsibility of Website Cell to issue user-ID and Password to each department / section on request, they
can modify their webpages but in case of any problem, Website Cell will help / modify the webpages.
11. . It is the responsibility of Website Cell to host the given information from department / section on given webpage
only. Responsibility of validity of information etc. lies with concern department / section only.

Recommended:

1. Provide information on timeliness (for example: August 2005; updated weekly; updated monthly, etc.)..
2 Provide a section indicating "What's New."
3. Provide a caution statement if link will lead to large pages or images.
4. Indicate restricted access where appropriate.
5. Avoid browser-specific terminology.
6. Provide link text that is clear without the link saying '**click here'** whenever hyperlinks are used.
7 Maintain visual consistency across related pages.
8. Provide a copyright statement (if and when appropriate).
9. Keep home pages short and simple.
10. Avoid using large graphics or too many graphics on a single page.
11. Provide navigational aids useful to your users (Link to Home, Table of
Contents, Next Page, etc.).
12. Maintain links to mentioned pages.
13. Make your Web pages easy to maintain for yourself and anyone who might maintain them in the future.

14. Avoid active links to pages that are in development. Place test or draft pages in your "test," "temp," or "old" subdirectory. Remember that nothing is private on the Internet: unlinked pages in your directory may be visible.
15 Check your finished page with a variety of browsers, monitors, and from both network and modem access points. It is also recommended that you check your page with a Web validation service.
16. Think of your users--test with primary user groups (which will be mix of users linking through our high-speed network, and users linking via much slower modems).
17 Conform to accepted, standard HTML codes.

Guidelines for Desktop Users

These guidelines are meant for all members of the SUK Network User Community and users of the University network.
Due to the increase in hacker activity on campus, University IT Policy has put together recommendations to strengthen desktop security.
The following recommendations include:
1. All desktop computers should have the latest version of antivirus such as Quick Heal and should retain the setting that schedules regular updates of virus definitions from the central server.
2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine.
Whenever possible, security policies should be set at the server level and applied to the desktop machines.
3. All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.
4. The password should be difficult to break. Password, defined as:
i. must be minimum of 6-8 characters in length
ii. must include at least one special characters such as ! $ % & * , . ? + - =
iii. must start and end with letters
iv. must not include the characters ' " `
v. must be new, not used before
vi. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No. etc.
vii. passwords should be changed periodically and also when suspected that it is known to others.
viii. Never use 'NOPASS' as your password
ix. Do not leave password blank and
x. Make it a point to change default passwords given by the software at the time of installation
5. The password for the user login should follow the same parameters outlined above.
6. The guest account should be disabled.

7. New machines with Windows should activate the built-in firewall.
8. All users should consider use of a personal firewall that generally comes along with the anti-virus software, if the OS does not have an in-built firewall.
9. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks).
When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.
10. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.
11. In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.
12. In addition to the above suggestions, INTERNET UNIT recommends a regular backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise.
Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.
13. If a machine is compromised, INTERNET UNIT will shut the port off. This will isolate the computer, until it is repaired as per the guidelines. At that time, the port will be turned back on.
14. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, INTERNET UNIT technical personnel can scan the servers for vulnerabilities upon request.

Appendix I

SHIVAJI UNIVERSITY, KOLHAPUR.
INTERNET UNIT

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/Net Access ID(user account)/email account , you agree to act in accordance with the IT policies and guidelines of Shivaji 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 the university. User can have a copy of the detailed document from the Intranet (viz.**http://www.SUK.ac.in/intranetchannel/SUK_ITpolicy.pdf**).

A Net Access ID is the combination of a username and a password whereby you gain access to

University computer systems, services, campus networks, and the internet.

I. 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 ID's will only be established for students, staff and faculty who are currently affiliated with the University.

Students, staff and faculty who leave the University will have their Net Access ID and associated files deleted.

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 Net Access ID related to the functions of that portfolio.

II. Limitations on the use of resources

On behalf of the University, INTERNET UNIT 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.

III. Computer Ethics and Etiquette

The User will not attempt to override or break the security of the University computers, networks, or machines/networks accessible there from. 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 University policy and applicable. Electronically available information

(1) may not contain copyrighted material or software unless the permission of the copyright owner has been obtained,
(2) may not violate University policy prohibiting sexual harassment,
(3) may not be used for commercial purposes,
(4) should not appear to represent the University without appropriate permission, or to represent others,
(5) may not appear to represent other organizations or companies,
(6) may not contain material which violates pornography laws, or algorithms or software which if transferred violate laws,
(7) may not contain scripts or code that could cause a security breach or permit use of resources in opposition to University policy, and
(8) WWW pages should clearly show identifying information of the owner of the page and we suggest that it also show date of last revision and an address (e-mail or postal) for correspondence. INTERNET UNIT equipment does not support use of scripting in individual pages.

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

INTERNET UNIT or COMPUTER CENTER 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
INTERNET UNIT/COMPUTER CENTER staff member in the process of helping the user in resolving their network/computer related problems. Although INTERNET UNIT/COMPUTER CENTER make a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email Account. In addition, INTERNET UNIT 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 INTERNET UNIT or COMPUTER CENTER, as part of SUK, harmless for any such liability or expenses. SUK retains the right to change and update these policies as required without notification to the User.

V. **Account Termination and Appeal Process**

Accounts on SUK 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, INTERNET UNIT will make an attempt to contact the user (at the phone number they have on file with INTERNET UNIT) and notify them of the action and the reason for the action. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the INTERNET UNIT of the same But, if the termination of account is on the grounds of willful breach of IT policies of the 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 Director INTERNET UNIT, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Appeals Board duly constituted by the university for this purpose to review the evidence and hear

reasons why an appeal should be considered. If the Appeals Board recommends revival of the account, it will be enabled. However, the Internet Unit of the Appeals Board is final and should not be contested.

Users may note that the University's Network Security System maintains a history of infractions, if any, for each user account. In case of any termination of 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 the appropriate University authorities.

Appendix II

SHIVAJI UNIVERSITY, KOLHAPUR.

INTERNET UNIT

REQUISITION FORM FOR E-MAIL ACCOUNT

1. Full Name : _____
2. Designation : _____
3. Dept./School
/Centre : _____
4. Office Telephone :_____
5. Please specify the E-mail Account Name you wish to have
6. Cell Number

Option @.unishivaji.ac.in

Date : Signature of the Applicant

User Counterfoil

The following email ID is created for Prof./Dr./Mr./Ms _____
_____
on _____.
@mail.unishivaji.ac.in

Signature on Behalf of Co-ordinator, INTERNET UNIT

Appendix III

SHIVAJI UNIVERSITY, KOLHAPUR.

INTERNET UNIT

Requisition Form for e-mail account / Wi-Fi access for Research Students (USE BLOCK LETTERS ONLY)

1. Full Name : _____
2. Programme of Study : _____
3. School : __ _____
4. Centre :____ _____
5. Year of Admission : _____
6. Semester : Monsoon/Winter
7. Permanent Address :

_____

_____

8. Local Address :

_____

_____

9. Telephone/Mobile No. if any: _____ _____
10. Identity Card No./ Library Card No. : _____

Declaration

The above information furnished by me is correct, and I undertake to abide by the rules and regulations of the University for proper use of email facility for my research work purpose.

Date : **SIGNATURE OF THE STUDENT**

_____ _____

_____

Application for email account recommended by

Signature Signature & Stamp of

Supervisor Chairperson/ Dean

Counterfoil

Mr./Ms. _____

***Email Account :_____@students.unishivaji.ac.in**

Signature

On behalf of Co-odinator

_____

* To be assigned by the INTERNET UNIT

SHIVAJI UNIVERSITY KOLHAPUR (SUK)

COMPUTER CENTER

CONFIDENTIALITY AGREEMENT

I _____ understand that as an employee of the Shivaji University Kolhapur (SUK) I will have access to computer/computer network, internet and data/information and confidential information of the data related to University. As an employee of the Shivaji University Kolhapur (SUK.), I undertake

a. To operate the communication through the email id assigned to me.

b. To maintain the confidentiality with respect to the password for email id and the Computer system assigned to me.

c. To take all possible steps to preserve strict confidentiality regarding any information to which I have access through my work.

d. Never to pass any information obtained as part of the duty/assigned work to anyone outside the section/department/University, unless I have been directed to do so by a more senior member of staff, and the reasons for doing so are clearly understood.

e. To keep all names, contact details and personal information secure.

I understand that any breach of the above will result in disciplinary action and/or may expose me to a suit for damages in a court of law.

Signed_____ Date_____

Witnessed by (please print) _____

Signature of witness _____Date_____