IT Policy

CONTENTS

CONTENTS

Appendix

IT Policies and Guidelines

1. Preamble

The Punyashlok Ahilyadevi Holkar Solapur University was established in 1st August 2004 as independent Maharashtra state University. Since its establishment the University steadily found its growth in all sectors including the IT infrastructure and services sector. The University makes best use of IT, including hardware, software and services, for its routine activities.

Since establishment the University realized that the IT infrastructure and internet are very vital for the growth. The IT products such as Computers, Printers, networking equipments, LCD devices, etc were procured based on the needs arising for academic and office activities. The University became member of National Knowledge Network (NKN) sponsored by the Ministry of Human Resource Development, Government of India, which provided the internet connectivity of 1 GBPS speed through its backbone across the country. This facility not only provides high speed internet connectivity to the students, research scholars and staff members of the University, but also provides abundant information resource needed for the students and research scholars.

The PAH Solapur University has various schools, with interrelated departments within each school. Every school has the computing centre with internet connectivity. Each school is connected to the centralized network. The administrative departments are also connected to this network.

University procured its own domain name and hosted the own website www.sus.ac.in. Under the Google Apps for Education all the students including students of affiliated colleges and staff members got institutional email IDs. This was a part of University's policy for speedy delivery of information to the students of the institution.

(i) With the increase in the number of users, the complexity also got increased. The vital resources like internet were being used in an uncontrolled manner. This may have the direct impact on the performance of internet because of the following reasons:

(ii) With no control on internet usage the prioritization of tasks does not happen. For example the tasks such as downloading of large files by a student and uploading of very important examination data will get same priority. This will hamper the high priority activities of the institution.

(iii) Certain user(s) can misuse the resource affecting the critical users and applications.

(iv) Since all the systems are interconnected, without any proper control and unauthorized users may creep into the privacy of other users and access the information from the computers of other users.

(v) Due to the inter connectivity virus can spread from one system to other system.

(vi) The computer, IT hardware and software purchased may not be competent enough to tackle exigencies due to lack of proper analysis and study carried out before procurement.

The other constraints that may affect the users across the institution, in particular the students and staff are:

(i) Limited capacity of internet bandwidth.

(ii) Limited and absolute resources such as computers, printers, IT laboratories, and other IT hardware and software.

(iii) Limited financial resources allocated to the, IT hardware, software and services.

Punyashlok Ahilyadevi Holkar Solapur University, Solapur ★

(iv) Limited availability of experts in specific software and IT services.

Realizing the above drawbacks the University took a decision to come out with a comprehensive IT policy, which could take into account all the above listed problems and constraints and would provide a viable solution to its users. The IT policy will provide broad guidelines for procurement and usage of university's IT infrastructure and computing facilities including computer hardware, peripherals, software, institutional email Ids, information resources, intranet and internet accessibility, which are collectively called "Information Technology (IT)". In view of these observations this document attempts to provide the IT policies and guidelines which would be relevant to this university.

Further, due to frequent changed and updated occurring in the Information Technology and information security sector, the policy governing information technology and information security should also need frequent changes and updated in its content, so as to fulfill the current requirements. Hence, the IT policy need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

This IT policy document will provide information regarding IT related activities and act as a guide to conduct acceptable actions and prohibits the violation of any defined activities. These guidelines are supposed to be used by all the stakeholders namely, students, research scholars, teaching faculty, non-teaching staff and any such person who is part or PAH Solapur University. The IT policy covers the hardware, software, campus network, internet maintenance and usage, database management, website, email ID creation and usage.

The University IT policy is applicable to all the entities and stake holders namely, centralized or individual administration of the IT technology, to all those administrative offices and departments which provide information services, the individuals who are the part of this University, provided by the university administration, schools and departments, the authorized resident or non-resident visitors who use or connect to the University network using their own hardware. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the university recognized Associations / Unions, or hostels and guest houses or residences wherever the network facility was provided by the university,

Further, the faculty, students, staff, departments, authorized visitors / visiting faculty and others who have permission to use the University's information technology infrastructure, must comply with the Guidelines. Any violations of IT policy defined in the IT policy document by any university member may result in disciplinary action. If the matter involves unlawful activity, then it may attract the legal action.

2. IT Policy for hardware

The IT policy for hardware covers all those devices which are categorized as hardware. They are computer CPU, monitor, keyboard, mouse, server, network devices, network cables, scanner, web camera, printer, external hard drives, external CD/DVD drives, laptop, LCD projectors and screens, overhead projectors, digital board, smart board, Xerox machine, CCTV camera and storage devices, etc.

2.1 Hardware procurement

The hardware procurement policy will describe the procedure for procurement of any hardware device for usage. The University should always prefer in purchasing high quality equipments and peripherals. The person who is responsible for purchase of such devices must make extensive survey of such devices from widely available internet surveys. The survey should be made keeping in mind the parameters such as quality of devices, durability, service terms (availability of local service centers may also be taken into

Punyashlok Ahilyadevi Holkar Solapur University account), turnaround time, warranty terms and conditions, post warranty maintenance conditions, customer satisfaction survey, pricing, etc. The top 5-10 such companies or brands may be chosen for purchasing the hardware. A clear configuration of minimum hardware must be specified, which should be available in almost all such selected hardware brands. A technical report based on above mentioned parameters must be submitted for further procurement of any hardware device. The user who wishes to acquire any hardware device should properly justify the requirement of such a device The Schools Departments/ sections can avoid the obstruction in regular functioning of work by procuring and storing the necessary peripherals which may be needed due to failure of such devices. Again such devices must be of standard quality from well known brands. Every department/School/section must maintain stock register with complete hardware configuration details. Any major device supplied by the vendors must be tested and certified by the appropriate technical committee framed by the University authority.

2.2 Hardware installation

Any major hardware device must be installed by technical person(s). The technician must provide appropriate initial training and instructions about proper usage of the installed device to all users of that equipment. The technical person must provide the phone numbers, email, IT Policy, PAH Solapur University addresses, website addresses, toll free numbers etc to the users to contact in case of any problem in operating with the device. The user must go through all the instructions provided in instruction manual for proper use of the device. The hardware must be installed in appropriate location with proper ventilation and enough space for comfortably operating with the device.

2.3 Hardware usage

The user(s) of any hardware equipments is/are solely responsible for proper use of devices. Users must follow the instructions provides by the technician and instructions provided in instruction manuals supplied along with the hardware device. The hardware device installed at certain location should not be removed or displaced without proper permission from higher authority. The user must be aware of who to contact in case of any problem faced during usage of device. The user also must have the knowledge of expiry of warranty period, in case the warranty needs to be extended. The hardware devices should be serviced only by authorized technical persons.

2.4 Hardware disposal

No device within warranty period should be disposed off. When a device, which is not covered tinder warranty, and found not working and not repairable, obsolete in technology, no more usable, may be disposed off. A proper disposable policy framed by the University must be followed.

3. IT policy for software

IT policy for Software covers all kind of software including operating system, system software, application software, diagnosis tools, antivirus, tools used for research and development, compilers, debuggers, network software, internet applications, web based applications, applications to operate specialized laboratory equipments. The software may have been developed in-house, may have been purchased from the vendors, may have been supplied along with the scientific equipments, or may he used based on contracts or under agreements.

3.1 Software procurement

The software procurement policy will describe the procedure for procurement of any software for usage. As much as possible stress must be given to procure and use open license software when such options are

Punyashlok Ahilyadevi Holkar Solapur University * India available and they are competent enough as compared to the commercially available software equivalent to it. In case of non-availability of such software or non-availability of specific features required by the user in open source software or finding difficulty in using the software as per the user needs, the user can recommend for purchase of commercial software with appropriate report explaining the above points. The person who is responsible for purchase of such software must make extensive survey of software from widely available internet surveys. The survey should be made keeping in mind the parameters such as quality of software, validity, current version, service terms, warranty terms and conditions, post warranty up gradation or maintenance conditions, customer satisfaction survey, pricing, etc. The user must also check whether the software is compatible with the hardware configuration (such as processor speed, memory space, storage space) on which the software would be installed. A technical report based on above mentioned parameters must be submitted for further procurement of such software. The user who wishes to acquire any software should properly justify the requirement of such software. Any software supplied by the vendors must be tested and certified by the appropriate technical committee framed by the University authority.

3.2 Software installation

Before installing any software the user of the computer on which the software has to be installed, has to carefully check the licensing policy. The user must ensure that no software is loaded in the computers which won't carry proper license. Proper instruction must be given to hardware vendors for avoiding installation of unauthorized software on the computers during its supply and installation. The user (Department head/head of the School in case of shared systems) of the system will be solely responsible for any unauthorized software or software without proper license, present on the computer used by him/her. When installing any new software a proper approval from higher authority must be taken. A register or record must he maintained specifying the details of software purchased such as license serial number, quantity of licenses warranty period, update policy from the supplier, price, supplier details, etc. The terms and conditions for open source software must also be properly read by the user to check whether it is free to use by the user for his/her intended usage. The users should also avoid the installation of software which is not used directly or indirectly for doing their routine work.

3.3 Software usage

The user of software has to check that the software used is not chocking the resources such as memory, CPU and storage devices, particularly when being used in network environment. The user must also be aware that the software will not harm the other software such as operating system, tools and other applications loaded in the computer. Whenever required, the user must update the latest versions, if available and authorized to get the updates.

3.4 Antivirus and updates

Every computer systems should have antivirus software installed and updated regularly. Every user should do regular scanning of computer using installed Antivirus. Pen drives should be scanned before use. Outsiders should not use pen drive without permission. Use of pen drives without scanning will be treated as data tampering activity.

4. IT policy for campus network

The IT policy for campus network is designed to protect the campus network and to be optimally used by the users of this network. This policy defines the standards for connecting computers, servers or other devices to the University's network. It also defines the standards in the design to minimize the potential exposure to University network and users from damages (including financial, loss of work, and loss of

Punyashlok Ahilyadevi Holkar Solapur University, Solapur ★

data).The campus network should be protected by strong firewall system, which avoids unsecured computer on the network and denies service attacks, viruses, Trojans, and other compromises to enter the university's campus network. Such attacks may damage the setups such as the loss of sensitive and confidential data, interruption of network services and damage to critical University internal systems. Such an attack may cause the damage to the public image of this institution. Therefore, individuals who connect computers, servers and other devices to the University network must follow specific standards and take specific actions.

4.1 Network connectivity

The users of the network may connect their devices to the campus network at appropriate connectivity points including voice/data jacks, and through approved wireless network access point, via a VPN or SSH tunnel, or through remote access mechanisms such as DSL, cable modems, and traditional modems over phone lines. The users much properly look into compatibility of ports before establishing the connections. Modifications or extensions to the network can cause undesired effects, including loss of connectivity. As a result, extending or modifying the University network must be done by following appropriate guidelines to carry out such extensions.

4.2 Network registration

Users of the university network must undergo secure authentication when connecting their computer to the campus network. To do such secure authentication users must have gateway software, which allowed the users to connect to the network. Such gateway software located at server will audit the network usage of every user. The campus network database will be maintaining the database of unique machine identification, network address and owner for the purposes of contacting the owner of a computer when it is necessary. Every computer and network device connected to the network, including a desktop computer has an associated owner or caretaker. For the sake of this policy, owners and caretakers are both referred to as owners. Such owners will be responsible for ensuring that their machines meet the relevant security standards and for managing the security of the equipment and the services that run on it. In schools and departments the responsibility of computer security and maintenance may be assigned to the University/Departmental Computing Coordinator or the University/Departmental Systems Administrator. In such situation it is possible that one owner would manage multiple departmental machines including his or her own personal computer. Every owner should be aware of who is responsible for maintaining his or her machine(s).

4.3 Network security

The network security policy will be applicable to all devices that get connected to the University network through standard university ports or through wireless services or through home and off campus connections. Users of University network must ensure that the software installed on their machines in no way breach or attack the security protection system of campus network servers and systems. They must also ensure that their computers won't have virus or malwares which can possibly attack and break the campus network firewall. The users of computers having sensitive or restricted Information should take additional measures for extra protections. Such users must seek appropriate expert consultation for providing additional security measures to protect such sensitive information. The University would possible have centralized secure network service for the entire University campus. Any individual user or Department should not run any service which may potentially cause the disruption in the smooth functioning of entire campus network. The list of such services includes email, DNS, DHCP, and domain registration etc.

The following procedures are adopted by the University IT authority to protect the campus network:

- Monitoring for external intruders - All network traffic which passes inside and goes outside the network is monitored by an intrusion detection system for any possibilities of compromises on network security.
- Scanning hosts on the network for suspicious anomalies University proposes a system which routinely scans the entire network, looking for any vulnerabilities. If any such possible vulnerability is found then extensive tests would be conducted and appropriate measures are taken to fix it.
- **Blocking harmful traffic** — If any security exposures or improper network traffic are found then University will take appropriate measures to avoid such possibilities. Such behaviour may be noticed by devices, which may exhibit the following activities:
    - ➢ exceptional Load imposed on a campus network service.
    - ➢ indications of pattern of network traffic that disrupts centrally provided services.
    - ➢ visibility of malicious network traffic with intention of scanning or attacking others.
    - ➢ exhibiting behaviour that may compromise host.

5. IT policy for internet and Intranet maintenance and usage

The IT infrastructure setup and maintenance unit (IT Department) of the University will be responsible for the internet and Intranet setup, control and maintenance of entire University campus. These network communications may be through wired network or through wireless network.

5.1 IP address allocation

The IP address allocation for any computer or any device in the network will happen through the IT department. The authorities in the IT department will systematically allocate balanced number of IP addresses to every department/School depending on the number of users in that Department/School. Any user is not authorized to change or re-allocate any IP addresses on their own without the permission from IT department. The IT department will keep record of the IP addresses by individual without permission is strictly prohibited. Everyone is bound by the IP allocation maintenance policy adopted by the ID department of the University. Similarly creating proxy servers, masking IP addresses, mapping of IP addresses etc. without appropriate permissions are restricted. IP addresses are one of the scarce resources. Hence IP addresses must be optimally used by the user. When the user no longer uses any network device with IP address assigned to it, such IP address must be surrendered to the IT department. Transferring IP addresses to some other device without knowledge and permission of IT department is not permitted.

5.2 Policy on usage of infra networks and network servers

The Individual users or users in departments/schools willing to use the campus network to run server software, such as, HTTP/Web server, SMTP server, FTP server, may do so with prior permission from the IT department. They have to make sure that such software will not cause disturbance or damage to any other network and software setup of campus.

Any user is responsible for any content found installed/stored on that user's machine. Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. Any act of impersonation of an authorized user while connecting to the campus network is treated to be an illegal activity of such user.

Punyashlok Ahilyadevi Holkar Solapur University, Solapur

5.3 Policy on individual usage of campus Internet

The University Internet facility is intended to use for organization's legitimate business requirements. Occasional and reasonable use of the Internet for personal purposes is regarded as acceptable subjected to the conditions that:

- Systems are not used for personal work during office working period
- Systems are not used for any private business or for any kind of commercial purposes
- Use of the system should not hamper the regular performance of the office duties
- This personal usage of the systems should not cost additional burden on the university
- User should not breach the prohibitions identified in this policy document. It can he noted that the University connects to the Internet through a dedicated leased Line at fixed costs. Hence the costs to the University remain the same irrespective of the amount of use. But the performance levels may decline as the line reaches optimal usage capacity.

5.4 Policy on prohibition of Internet usage

The University prohibits use of its Internet network for the transmitting, retrieving or storing of any communications or images which are:

- Harassment — It is unwanted conduct (including insults and jokes') which relates to gender, sexual orientation, race, religion, disability or other similar issues
- Defamatory - Defamation is the publication, of any content which directly or indirectly affects the reputation of a person or an organization
- Copyright - The owner of any copyright material will have exclusive right to decide on how that material might be copied and used. There will not be any permission to transmit copyright material without written permission from its owner
- Pornographic - Any material of a sexual nature is treated as pornographic. Visiting pornographic sites, downloading its content or transmitting any pornographic content over campus network is prohibited.

Other than the above activities, the following conducts are also prohibited:

- Use of the University Internet facilities to deliberately propagate computer viruses, worms, Trojan horses or trap door programs is prohibited.
- Use of the University Internet facilities for the purpose of disabling or overloading any computer system or network, or to attempting to disable, defeat or circumvent any system, which is established to protect the privacy or security of another user is prohibited.
- Any additional Internet or e-mail related software should not be installed, configuration of existing software should not be changed by users without permission of IT department.
- Use of the campus Internet facilities to download, upload or distribute pirated software is prohibited.
- Use of the campus Internet facilities to download entertainment software of games or to play games over the Internet is prohibited.

6. IT policy for Database Management

This Policy relates to the management of databases generated by the different applications used for regular activities of the University, which include administrative, finance, examination, academic etc. Data is one of the important resources which are generated out of the computerization of regular

University activities/transactions. Providing security and maintaining its integrity is very vital for the University. The data may be generated from the applications which are purchased from the third party or developed internally. Such data may exist in any advanced RDBMS or may be in spreadsheets. University has exclusive ownership of the all such data or database which is being generated by the users of applications hosted for or by the PAH Solapur University. Such data may also be generated by third party applications on which the University may not claim ownership, but the University administration have right to collect information from other users for any specific purpose. The data may be generated by different departments depending on the kind of their requirements. In such case the person. who would be an authority of University having permission to collect such information, will be the custodian of that data. Any such custodian will use the data exclusively for the purpose of University and neither have authority to use it for any personal reasons not authorized to deliver it to third party with or without the intention of personal benefit. In the centralized database system the database administrator will be the custodian of the data. Any data generated in electronic form or in hard copy cannot be decimated to any external agency by individuals without proper permission. When such information has to be sent to Government or any other finding or statutory body, it has to be channelled through appropriate authority. This condition may not be applicable to sharing of research data in case of collaborative or joint research projects. But such research projects must be in the knowledge of University authority. Any kind of tampering of data by any individual is strictly prohibited. Any of the following activity may be treated as tampering of data, but it may not be limited to these activities only.

- Unauthorized insertion, modification or deletion of data causing errors in the data either through use of software or by directly accessing database.
- Dropping, renaming or causing damage to any component or element of any database by any individual with malicious intention.
- Causing any damage to the storage device such as hard disc, CD/DVD, pen drive, memory card etc having the data.
- Damaging data in cloud, denying access to the Users of data available in the cloud, redirecting the access of data to different database in cloud.
- Breaking the security system of data files, databases, database servers or database management systems I software.

7. Backup of data

The primary causes of data loss are computer failure or crash, virus infection, software failure, theft, accidental deletion etc. Backup copies help to restore data. Therefore every user should keep regular backups of their vital data. Also backups are essential before formatting any computer due to genuine reason. Backups can be kept securely on other storage devices such as pen drives, CDs, external hard drives etc.

8. IT policy for website

University is actively using IT resources like websites, email services, social sites, short messaging services and other electronic communication systems for communicating and interacting with the users of the system. These types of communication has potentially reduced the cost incurred by institution and speeded the communication. Since most of the users would be dependent in the information provided through these communications, effectively maintaining and updating the information on websites would be one of the duties of the University.

Punyashlok Ahilyadevi Holkar Solapur University, Solapur *

8.1 Policy for web content users

Following are some of the policy guidelines and notice for the users of PAH Solapur University official website.

- All the content of website, data available in the website, images and files available in the website domain are exclusive property of PAH Solapur University.
- PAH Solapur University will always make efforts to maintain reliable, accurate, correct and up-to-date information over its website. If any erroneous information is found, same may be brought to the notice of University authority.
- The University website may contain links to the external sites, not owned by the University. University will not be responsible for error in opening such websites, relevant information missing over there, unexpected content found there.
- The content of University website such as images of persons, videos of events, logos, University related exclusive information, University policies are either property of PAH Solapur University or being used by University with appropriate permission. Use of the above content without permission for any commercial purpose may attract copyright violation and such user may be prosecuted under copyright act.
- Users may view or download the information or content of the website. Whenever the information is sought from the user through appropriate data entry applications, users may provide information correct to their knowledge. Entering false, misleading and unnecessary information, hacking the website, directly accessing the databases bypassing the website forms and applications are treated as unlawful activity.
- University will not be responsible for the any type of losses to the users due to breakdown or unavailability of website, because of any unavoidable circumstances, such as failure of web server, failure of internet, frequent disconnection to website. These events are beyond the control of University.

8.2 Policy for web content contributors

The website contributors are those categories of users who have authority to upload, update, insert or delete the content of the website. Apart from the following guidelines, they are also bound by the rules and guidelines listed for the website users.

- The official University website www.sus.ac.in has been developed with a very systematic approach, where the content is clearly categorized based on their type and as much as possible not content will overlap in any multiple sections. An easy way of methodology is provided for updating the content of the website. The website content maintenance and updating can be done through decentralized access.
- Since the content of entire website would be generated through decentralized updating and deleting mechanism, maintenance of correct, accurate, appropriate information would be the responsibility of individual(s) who is/are authorized for that particular content. Before updating any content onto the website appropriate approval must be obtained from their higher authority.
- The contributors of the web content must fix the validity period for any content uploaded by them. After the expiry of validity period the content should no longer be available on the website. If still such content appears on the website, then the contributor should remove it. The contributor must also ensure that no hyperlinks exist in their content domain which will direct to nonexistent websites or redirect to wrong websites.

Punyashlok Ahilyadevi Holkar Solapur University, Solapur ★

- The web content contributors should not upload any offensive content, content against the policies of University, content contradicting the official stand of the University, personal opinion over any official stand etc.
- The respective department head/Director of the school / Section head will be responsible for any content uploaded by any official of respect I've department / School /section.

8.3 Policy for website and content developers

Web developers are the one who have the skill of website development and involved in the development of University website. They will be responsible for design of the overall website, creating the web content structure, organization of its content, adding graphics and images during its design, writing codes for its background functionalities, providing rich features to the website etc. The web content developers may be external agencies hired by the University for One Time Development. University may get extended their services whenever there is need for revision or modification in the website design. The primary aim of the web developers must be to provide a stable website as per the requirements of users. They are supposed to use the standard scripting languages and database such as Hyper Text Markup Language (HTML), Ajax, Java Script, and PHP (Hypertext Pre-processing), Cascading Style Sheets (CSS), and MySQL during the development of website. The orientation must he for using open source scripting tools and databases. The hosting of website over the servers should not attract additional cot on the University such as cost involved in purchasing website development tool or database tool. The designers should not use unsecure database files such as Excel sheets or flat files for storage and retrieval of data. The scripts not related to the website such as batch scripts, other processes, any other applications not related to website and not used by the PAH Solapur University should not exist on the web server. The database applications required by departments/schools may be uploaded with permission from the higher authority.

8.4 Policy for website administrators

Website administrator is employee of PAH Solapur University whose role will be to manage of entire website. Website administrator manages the operational component of website, The web operations are providing access to website, verifying the content of the website to check for up-to-date content in it, and any such related operations. In emergency situations hacking, breakdown or attack on website, the website administrator must be able to effectively and rapidly replace the website with the message stating non-availability of website for temporary reasons or redirect them to some other website. The website administrator must also be able to change, disable, activate, deactivate, delete, add any website content as and when any such request comes from the higher authority. Website administrator should follow proper naming convention for the files, images, and other web contents which would be uploaded into the website. He/she should also be able to give proper identification code or login details for every website contributor with proper authentication procedure. Website administrators should monitor website content to ensure appropriate use and compliance with IT policy and ensure that Web developers and content contributors at all levels follow all policies in described in the previous sections.

8.5 Other policy guidelines related to website

Web media is the content such as audio, video, multimedia files and other file types excluding the web pages. Web media files are usually very large in the size and require more storage space and higher bandwidth for uploading and downloading. Because its large usage of internet resource some guidelines are described in this section to manage web media content in website. The department/School/section heads, in consultation with their subordinates must plan for maintaining rich multimedia content in their gallery. Such media content may be photographs, short videos, audios, etc. Before uploading such content proper approval must be obtained from the higher authority. Since the web media require large storage space the IT department will fix the space quota for each department/school/section depending on their needs. On requirement the department/school/section may demand additional space by quoting appropriate reason for such type of need. Such needs may arise whenever they plan for broadcasting the video lectures, special events and programmes, Live presentations, which may be of temporary in nature. Streaming and delivery of any Web media on the University network will be monitored and fine tuned to ensure reliable content delivery based on the capabilities of the existing network infrastructure. Needs for system specifications, network and bandwidth information can he communicated in advance to the IT department so as to make appropriate arrangement for smooth streaming of event.

9. IT policy for email ID creation and usage

The purpose of IT policy for email ID creation and usage is to facilitate the users to identify themselves with PAH Solapur University while communicating with external entities, to provide unique identification for communication and to help in utilization of internal resources.

9.1 Policy for email ID creation

The PAH Solapur University has partnered with Google for the implementation of Google Apps for Education. The prime product of this is institutional ids email. PAH Solapur University has adopted a systematic procedure for provisioning email addresses for all its stake holders including employees, teachers, students in campus and students of affiliated institution under the domain sus.ac.in. A proper segmentation has been provided for all users like Administrative staff, teaching faculty, temporary teaching faculty, non-teaching faculty, students in campus, students of affiliated colleges etc. In future it intends to provide its institutional email IDs to all the students to be admitted to the PG departments and affiliated colleges. For all employees in of the University campus the naming convention followed for their email id is <first_name_initial><middle_name_initial><sername>gsus.ac.in and for the students of campus and affiliated colleges the ID must contain above information along with their course and/or year of admission and/or college abbreviation. When new email addresses are created the administrator must follow the convention of their categorization. As soon as new employee joined or new students join the University the administrator shall initiate the process of obtaining approval for provisioning the institutional email addresses for new entrants. On approval same may be provided and issues to respective user.

9.2 Policy for email ID usage

The University institutional email ID is the property of PAH Solapur University and it shall not to be used for the creation or distribution of any disruptive and/or offensive messages, including offensive comments about race, disabilities, gender, hair colour, age, pornography, sexual orientation, political beliefs, religious beliefs and practice, or national origin. Anyone who receives any emails with this content from any PAH Solapur University institutional email ID should report the matter to University authority.

Use of reasonable amount of University details, such as University name, Department / School / Section name, address, phone numbers, etc for the personal emails are permitted. Employees must save official emails separately from the personal emails when saved on the storage device. Sending joke emails from a institutional email account is prohibited. Virus or other malware warnings and mass mailings from institutional email account shall be approved by higher authority before using it.

The PAH Solapur University encourages its institutional email address users to adapt the ethics for appropriate use of email, and to avoid any misconduct. Users should follow following guidelines.

- Keep passwords undisclosed and secure.

Punyashlok Ahilyadevi Holkar Solapur University, Solapur *

- ➢ Every email may he electronically scanned for obscene, indecent and illegal remarks. Hence should not use such content in emails.
- ➢ Should not express themselves in a way that could be defamatory.
- ➢ Users should not transmit attachments of larger size, especially graphic and multimedia files. If really necessary same may be brought to notice of authority before transmitting.
- ➢ User should not give out their email address to any external sources, who found to be untrustworthy.
- ➢ Institutional users should not send confidential information over e-mail to unauthorized recipients.

10. Responsibilities of IT Department

The IT department of University will consist of a senior IT head having overall expertise of hardware, software, network and internet. He/she will be assisted by one or two IT assistants who could implement the plans and instructions given by the IT head. The IT department will have all tools and machines required for extension works, troubleshooting and maintenance of campus IT products such as hardware devices, peripherals, software tools, local area network and internet.

- Management of Campus Network Backbone: The campus network once established, will interconnect all the departments/schools with the centralized resources such as servers, databases etc. IT department will be responsible for smooth functioning of this network backbone.
- Logical and physical separation of departments: For the purpose of optimal utilization of network resources such as OFC networks, bandwidth, routers etc the IT department has responsibility to logically and physically divide these resources optimally among different departments/Schools depending on the number of users. The IT department will have to provide justice to everyone in making provision for internet resources. They have to see to it that everyone get fair bandwidth and wherever there is need for excessive bandwidth, proper arrangements need to be made by fairly looking into the requirements. The IT department will also be responsible for the planning and executing the extended cabling in campus and within the buildings.
- IP address allocation: IP addresses are one of the scarce resources which need more attention in allocation. Where ever genuine request comes for static IP addresses, same may be allocated by obtaining approval from the higher authority. NAT addressing can be used for providing enough IP addresses to the departments/schools. While allocating IP addresses the future requirements of the Departments/Schools has to be considered and accordingly the provisions should be made.
- Activity monitoring: IT department will be responsible to keep watch on the activities happening across entire campus network using appropriate firewall software. The monitoring can be made on activities like checking unauthorized users, sending span mails by users, downloading and uploading unusually large size files, visiting the harmful and adult websites, skewed usage of internet bandwidth, unauthorized access to University database, hackers of University website, etc. If any of the above activity found then necessary action must be taken to prevent further activity and details of activity must he reported to higher authority for further disciplinary action. The IT department will not have authority to open any users' email addresses or access any users' emails without users' permission.
- Management of institutional email ID: University employees and students extensively use the institutional email IDs for their regular communication. They are unequally identified globally by the institutional email IDs. Whenever a new user (employee or student) is added to the institution the IT department must make provision for his/her email ID. Convention for creating email IDs must strictly be followed. Once email ID is created, its authorized user must be intimated and user must be forced to change the login password. Whenever an employee leaves the organization or retires from service or dies, the email ID of such employee must be withdrawn. IT department

should also see to it that no one misuse the institutional email ID for their personal gain or with the intention to bring bad name to the institution.

- Installation and management of wireless network: In the current era of wireless communication usage of wireless devices such as smart phones, laptops and tablets are increasing day-by-day. On establishment of campus internet network, wireless internet facility must be made available to users who opt to use internet using their wireless devices. The usage must start with appropriate login process. At any instance any authorized user should not be able to login in more than one instance.
- Renewal of licenses: IT department will be responsible for the renewal of any licenses, lease periods, warranty period of IT resources such as data servers and routers, domain name and domain space, etc related to the entire University campus. The renewal must happen before the expiry period. Before proceeding for any renewal permission must be obtained from the higher authority.

11. Responsibilities of University Departments/Schools

University Departments/Sections/Schools comprise the major users of the University IT resources. They play important role in the usage of IT resources. Following are the few guidelines for optimal utilization of IT resources by the users from these sectors:

- IT resource management: Every user/employee and head of respective department/School shall be responsible for maintenance of IT resources. If any device is found to be faulty same must be reported to the IT department to get it serviced. Proper stock register must be maintained for all the IT hardware devices and software tools. When any device is found to be unusable, same may be written off with approval from the higher authority. If any of the e-waste has to be disposed off, appropriate disposal methodology has to be followed to avoid the hazard in the environment.
- Updating web content: www.sus.ac.in Website is logically divided based on the Departments/Schools/Sections. Every authorized user could login and update the information related to respective sections. The responsibilities of maintaining up-to-date information over the website will be with individuals concerned to respective Departments / Schools / Sections. The head of related Department must cheek the content before providing approval. Since the approval issue system is digital, care must be taken regarding the content of the matter to be uploaded into website. They are also responsible for removing the old and absolute information from the official website.
- Email ID usage: Every user is provided with the institutional email IDs. Everyone has will be responsible for positive use of these institutional email [Ds. The TDs created for officers of the institution should be used for official purposes only. When there is no need of any official email ID same may he surrendered to the IT department. It will be the responsibility of the Departments/Schools head to get email ID from the IT department for the newly joined employees and students and delete the email IDs of employees who quit the organization. Users should not disclose password of their institutional email ID to anyone else in any circumstances.
- Internet resource usage: The Department/School head shall have a broader monitoring system to check proper usage of internet, even though the IT department will be responsible for detailed monitoring of internet usage. Students and users must be instructed to avoid downloading of larger files, particularly the files not related tc academic, research or their work. Users must also be instructed to avoid visiting the social network websites, chatting sites, news forums, entertainment, adult sites, etc. If anyone is found violating the instructions, appropriate action must be taken to suspend/withdraw the user login from such user.

Punyashlok Ahilyadevi Holkar Solapur University, Solapur ★

- IT infrastructure expansions: Any Department/School willing to expand the IT infrastructure such as network, computer lab infrastructure must bring same to the notice of IT department regarding proposed expansion activity. Such expansion should not affect the normal activities of other Departments/Schools and should not overburden the existing campus network/internet bandwidth. Unnecessary expansions must not be taken up by any Department/School.
- Use of legal software/hardware: The Department/School heads must be strictly instruct the users not to use illegal/unlicensed software and hardware devices. Use, of any software for hacking websites, hacking email IDs, steeling classified information from any website, steeling personal information of any individual, destroying the software set and operating system of the PCs, spreading viruses, sending spam emails, attacking the University servers, intentionally or

Appendix A

PAH Solapur University, Solapur.
IT Department

Request for Allocation of IP Address

1. Name of Department/School/Section :

2. Name and Designation of Head :

3. Host name :
(for which IP address to be allocated)

4. IP type (Static/Dynamic/Any) :

5. Host Details (Brand / Configuration) :

6. MAC/Physical/Adapter address :

7. Operating System(s) :

8. Network/Internet Apps in system :

9. Other applications in system :

10. Name of Antivirus & expiry :

11 . Is system a serve?? If yes give details :

12. Is system connected to campus net? :

13. Who use the system? :

14. IP allocation purpose :

15. Required temporarily i permanently? :

Date :   Sign. of user (if any)   Sign. Of Head/Director

For Official Use only

IP address allocated/not allocated

If static IP allocated then IP address:

Remarks:

Sign. of technical person
Head

Sign. of IT Dept.

Appendix B

PAH Solapur University, Solapur.

IT Department

Request for Allocation of Institutional Email Address

1. Name of Department/School/Section :

2. Name and Designation of Head :

3. Email ID requested :

(if multiple Ids requested then list may be attached. Email ID format to be followed)

4. Details of the ID User :

i. First Name :
ii. Middle Name :
iii. Last Name :
iv. Class/Designation :
v. Date of birth :
vi. Date of joining :
vii. User type (student/teacher/staff) :

5. Alternate email ID of the user :

6. User phone number :

7. Validity period, if any :

8. Does user already have institutional email ID? :

if Yes

i. Details of other email ID(s) :
ii. Why additional Ill requested :
iii.

Date : Sign. of user (if any) Sign. of Head/Director

For Official Use only

Email address allocated I not allocated

Email ID :

Remarks :

Sign. of technical person Head

Sign. of IT Dept.

Ahilyadevi Holkar Solapur University, Solapur * Punyashlok

Appendix C

PAH Solapur University, Solapur.
IT Department

Request for Allocation of Internet Access ID

1. Name of Department/School/Section :

2. Name and Designation of Head :

3. User ID (Institutional email ID) :

4. Details of the ID User :

i. First Name :
ii. Middle Name :
iii. Last Name :
iv. Class/Designation :
v. Date of birth :
vi. Date of joining :
vii. User type (student/teacher/stall) :

5. Alternate email ID of the user :

6. User phone number :

7. Validity period, if any :

Date : Sign. of user (if any) Sign. of Head/Director

For Official Use only

Internet access approved/not approved

Email ID :

Validity period (if any) from : to :

Data access limitation (quota, if any, per day/week/month/year) :

Accessing time (if any) between Hrs. to Hrs.

Remarks :

Sign. of technical person
Head

Sign. of IT Dept.

Punyashlok Ahilyadevi Holkar Solapur University, Solapur ★

Appendix D

PAH Solapur University, Solapur.
IT Department

Request for Wi-Fi access account

I. Name of Department/School/Section :

2, Name and Designation of l-lead :

3. User ID requested :

4. Details of the ID User :

i. First Name :
ii. Middle Name :
iii. Last Name :
iv. Class/Designation :
v. Date of birth :
vi. Date of joining :
vii. User type (student/teacher/stall') :

5. Alternate email ID of the user :

6. User phone number :

7. Validity period, if any :

Date : Sign. of user (if any) Sign. of Head/Director

For Official Use only

Wi-Fi Internet access approved/not approved

Email ID :

Validity period (if any) from : to :

Data access limitation (quota, if any, per day/week/month/year)

Accessing time (if any) between Hrs. to Hrs.

Remarks. :

Sign. of technical person Sign. of IT Dept.
Head

Punyashlok Ahilyadevi Holkar Solapur University, Solapur ★

व्यवस्थापन परिषद
विषय क्रमांक (21(5))
दिनांक :- 31 MAY 2021

विषय क्र. २१(५) IT Policy व Research Policy बाबत मा. कुलगुरु महोदयांनी महाराष्ट्र सार्वजनिक विद्यापीठ अधिनियम, २०१६ कलम १२ (७) नुसार व्यवस्थापन परिषदेच्या वतीने केलेली कार्यवाही माहितीस्तव.

सदर विषयासंदर्भात तातडीची बाब लक्षात घेता, मा.कुलगुरु महोदयांनी केलेल्या कार्यवाहीची नोंद घेण्यात आली असून, सर्वानुमते खालीलप्रमाणे ठराव पारित करण्यात आला.

ठराव : IT Policy व Research Policy बाबत तातडीची बाब म्हणून, मा.कुलगुरु महोदयांनी महाराष्ट्र सार्वजनिक विद्यापीठ अधिनियम, २०१६ कलम १२ (७) अन्वये व्यवस्थापन परिषदेच्या वतीने केलेल्या कार्यवाहीची नोंद घेण्यात आली.

पुण्यश्लोक अहिल्यादेवी होळकर सोलापूर विद्यापीठ, सोलापूर ★