Dev Sanskriti Vishwavidyalaya

IT Policy

INFORMATION TECHNOLOGY INFRASTRUCTURE USAGE POLICY

Introduction

Students, Teaching Staff and Non - Teaching Staff, Management, Visiting Guests and Research Fellowship Members of Dev Sanskriti Vishwavidyalaya availing computing, networking, and IT facilities are expected to abide by the following rules, which are intended to preserve the utility and flexibility of the system and protect the privacy and work of students and faculty.

General Rules

1. Students, Teaching and Non - Teaching Staff, Management and visiting Guests and Research Fellowship Members are authorized to use the computing, networking, and other IT facilities for academic purposes, official university business and for personal purposes as long as such use does not violate any law or any university policy.

2. The University prohibits its users from gaining or enabling unauthorized access to forbidden IT resource on the University network. Any such attempt will not only be the violation of University Policy but might also violate national and international cyber laws, provisions under The Information Technology Act of India and infringe the principals of National Cyber Security Policy. It might even subject the user to civil or criminal liability, or both. However, the University reserves all the rights to access and analyze the IT resource and Information for any legal and/ or institutionally provisioned operation, on its own or through its affiliates.

3. The University prohibits its users from sending, viewing or downloading fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or content(s) that are a violation of applicable law or the University policy. Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful e.g. when such content is received through e-Mail etc. As a generalized policy, any contribution towards the destruction or distortion of congenial academic or work environment, is prohibited.

4. Users must not violate various IPR and copyright law(s), and licensing policies as associated with copyrighted materials and software. Any unlawful file- sharing, use of any form of illegal or pirated or un-licensed software, on the University's IT resources (including individually owned IT resource being used under Institutional IT privileges) is strictly prohibited and any such act shall constitute a violation of the University policy.

5. By agreeing to abide by the terms of use of various online media forums, the users are expected to adhere with the norms as prescribed by respective social networking websites, mailing lists, chat rooms, blogs. Unless a user has proper authorization, no user should attempt to gain access to information and disclose the same to self or other unauthorized users. The broader concept of data privacy must be honored by each user.

6. No user should attempt to vandalize, damage or change any data inappropriately, whether by accident or deliberately. The basic notion of trustworthiness of information resources must be preserved by all of its users. Any interference, disruption or encroachment in the University IT resources shall be a clear violation of the University policy.

7. No user should attempt to affect the availability of IT resource, whether accidently or deliberately.

8. As a part of certain investigation procedures, the University may be required to provide its IT information, resource and/ or records, in part or full, to third parties. Also, for proper monitoring and optimal utilization of available University IT resources, the University may review, analyze and audit its information records, without any prior notice to its Users. Further, the University may also seek services from third-party service providers. Accordingly, the users can only have reasonable expectation of privacy on the University's IT resources.

9. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems.

10. No food or drink is permitted in the laboratories. Also making noise either through games/music/movies or talking and/ or singing loudly (the list is not exhaustive) is prohibited.

11. Violations of any University policy or policies will be treated as an academic misconduct, misdemeanor or indiscipline. Depending upon the nature of the violation, the University authorities might take an action.

Responsibilities of University COMPUTER LAB

A. Maintenance of Computer Hardware & Peripherals
COMPUTER LAB is responsible for maintenance of the university owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Cell.

B. Installation of Un-authorized Software
COMPUTER LAB or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

C. Reporting incidents related to Network Operations
When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the COMPUTER LAB by IT Cell. After taking necessary corrective action, the COMPUTER LAB or service engineers should inform IT Cell about the same, so that the port can be turned on by them.

D. Rebuilding the Computer System
When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, dynamic or static IP address, network Mask, gateway as it was having earlier. Further, after installing the OS, all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded

from the net. Further, before reformatting the hard disk, dump of only the data files should be taken for restoring it back, after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

E. Coordination with IT staff

Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the network or the software installed or hardware malfunctioning Computer LAB /service engineer may coordinate with IT staff to resolve the problem with joint effort. This task should not be left to the individual user.

Guidelines for Desktop Users

These guidelines are meant for all members of the DEV SANSKRITI VISHWAVIDYALAYA Network User Community and users of the University network. Due to the increase in hacking activities on campus, the University IT Policy has put together recommendations to strengthen desktop security.
The security recommendations include the following:

1. All desktop computers should have the latest version of Windows such as
Windows 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 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 punctuation 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.

5. passwords should be changed periodically and also when suspected that it is known to others.

i. Never use ‘NOPASS’ as your password
ii. Do not leave password blank and Make it a point to change default passwords given by the software at the time of installation

6. The password for the user login should follow the same parameters outlined above.

7. The guest account should be disabled.

8. New machines with Windows 10 should activate the built-in firewall.

9. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.

10. All the software on the compromised computer systems should be re-installed from scratch

11. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.

12. 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.

13. In addition to the above suggestions, IT Cell 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 a hacker compromise. Backing up data on a regular basis (daily and/or at least weekly) will lessen the damage caused by the loss of a machine.

14. If a machine is compromised, IT Cell 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.

15. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, IT Cell technical personnel can scan the servers for vulnerabilities upon request.

Date: **Signature:**