વિષય: એન.એ.યુ. આઈ.ટી. પોલીસીની મંજુરી અંગે

જાહેરનામું નં. ૬૪૫/૨૦૧૮

આથી સબંધકર્તા સર્વેને જણાવવામાં આવે છે કે, તા. ૫-૭-૨૦૧૮ ના રોજ નવસારી ખાતે મળેલ સંચાલક મંડળની ૪૦મી બેઠકની કાર્યનોંધના મુદ્દા નં. ૪૦.૦૩ થી નીચેની વિગતે ઠરાવ કરેલ છે.

"આથી ઠરાવ કરવામાં આવે છે કે, નવસારી કૃષિ યુનીવર્સીટીમાં આઈ.ટી. સેવાઓના અમલીકરણ માટે નવસારી કૃષિ યુનીવર્સીટી આઈટી પોલીસી Appendix-40.03(i)to(x) મંજુર કરી કાર્યવન્તીત કરવા માટે પરવાનગી આપવામાં આવે છે."

નિયામક
ઈન્ફોર્મેશન ટેકનોલોજી
નવસારી કૃષિ યુનિવર્સિટી
નવસારી – ૩૯૬ ૪૫૦.

જા.નં.ન.કૃ.યુ./આઈટી/૧૬૪/૨૦૧૮
તા. ૦૧/૦૮/૨૦૧૮

નકલ સવિનય રવાના:

(૧) સંચાલક મંડળના તમામ સભ્યશ્રીઓ તરફ
(૨) યુનીવર્સીટીના તમામ અધિકારીશ્રીઓ તરફ
(3) તમામ યુનિટ/સબ યુનિટ અધિકારીશ્રીઓ તરફ
(૪) કુલસચિવ વિભાગની બોર્ડ ઓફ મેનેજમેંટ શાખા તરફ (૦૫ નકલમાં)
(૫) રહસ્ય સચીવશ્રી [માન. કુલપતિશ્રી/કુલસચિવશ્રી] તરફ
(૬) જાહેરનામાં ફાઈલ

Policy of Information Technology Resources and Services of NAU – 2017

Abbreviation

- NAU – Navsari Agricultural University
- IT – Information Technology
- UTP - Unshielded Twisted Pair
- VPN – Virtual Private Network
- ERP – Enterprise Resource Planning
- NOC – No Objection Certificate

Scope of Policy

This policy governs the usage of IT resources and services from an end user's perspective.

Objective

The objective of this policy is to ensure proper access and usageof IT resources and services by the end users.

1. Role and Responsibilities

Role to be performed by the IT Cell for implementing infrastructure and services:

1. To develop and implement different IT services across the University.
2. Administration of Internet services across the University.
3. Developing / procuring / administration of various required software for University automation process on regular basis.

Responsibilities need to be performed by the end user:

1. Responsible for carrying out functional aspect of the IT services.
2. The responsibility of maintenance and troubleshooting of desktop computers, all in one computers, laptop/notebook, printers, scanners and other related peripherals shall be carried out by the respective end user/department/unit.

2. Hardware Resources Policy

2.1 Introduction

The IT hardware resources include desktop computers, all in one computers, servers, laptop/notebook computers, thin client computers, wireless access points, Wireless adapters, network switch/hub, printers, scanners and other computer peripheral devices etc.

NAVSARI AGRICULTURAL UNIVERSITY * NAVSARI.* कृषिमूला ऋद्धिः Navsari Agricultural University Navsari

2.2 Scope of IT Hardware

The IT cell is responsible for buying and deploying the necessary IT hardware resources for providing IT services. The internet connectivity services shall be procured / deploy / carried out by IT Cell subject to the budgetary provisions.

Respective units and departments are responsible for procuring and maintaining hardware's like desktop computers, all in one computers, servers, laptop/notebook, printers, and scanners through appropriate university laid down purchase process.

Maintenance of network switch, rack, wireless routers, UTP cable, I/O box installed in respective units will be maintain by IT Cell. Cost of maintenance / replacement / extension will be executed by respective units through appropriate university laid down purchase process.

2.3 General Guidelines for end user

1. Computers shall normally be used only for executing University work. Users shall exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.
2. Users shall ensure that updated licensed antivirus / scanning software is running in the systems.
3. Users shall abide by instructions or procedures as directed by the IT Cell from time to time.
4. End user cannot deploy / install network equipment in university network without prior permission of IT Cell.

2.4 Advisory Guide

1. Software installed on IT resources must be licensed software.

3. NAU IT Software Resources Policy and Guidelines

3.1 Introduction

This policy provides guidelines for the use of software for all employees/students within the NAU to ensure appropriate usageof it. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

3.2 General Guidelines

1. Users shall not copy or install any software on desktop devices including privately owned shareware and freeware without the approval of the IT Cell.
2. Users shall not share their accounts, passwords or similar information or devices which is used for identification and authorization purposes.

NAVSARI AGRICULTURAL UNIVERSITY
कृषिमूला ऋद्धिः
Navsari Agricultural University
Navsari
* NAVSARI. *

3. All software installation is to be carried out by end user only.
4. End Users should not use any VPN and Third party Software that exploit firewall and make NAU network vulnerable to the network attacks at NAU. If end user found out to carry out such malpractices than their account will be blocked / suspended on permanent basis.
5. End user is solely responsible for user level software Issues.

3.3 Advisory Guidelines

1. Users shall use strong password to defend against attacks.
2. Users shall not use pirated software.

4. Network Policy and Guidelines

4.1 Introduction

Navsari Agricultural University (NAU) Network is a wide area network that is comprised of buildings located at Navsari campus as well as that of remote stations using VPN technology. All the IT services delivered through this network medium from NAU server room. NAU network can be accessed through two modes wired network and wireless network. The policy for accessing wired and wireless network is as per given below.

4.2 Wired Network

Wired network comprises of fiber optic cable connectivity from server room to switch located at various buildings, from there the network is extended to switches or I/O box. The different roles and responsibilities for wired network are as per given below.

4.2.1 Responsibility of IT Cell

1. IT Cell is responsible to manage and administration of NAU wired network.
2. IT cell is responsible for Network connectivity up to department level.
3. The Network connectivity and the troubleshooting will be carried out by IT Cell subject to guidelines issued time by time.
4. Alteration / maintenance / extension activities in entire NAU network will be only carried out in the supervision of IT Cell.
5. IT Cell shall not responsible for failure in IT devices due to electricity issues at any place.

4.2.2 Responsibility of Unit / End User

1. The power supply to network equipment's and rack will be the sole responsibility of respective units.

2. Unit is not allowed to make changes in the network cabling at their premise without the consent of IT Cell and such activity will be treated as a network tempering.
3. No end user is allowed to share their internet service account with anyone.
4. Users shall not undertake any activity through any website or applications which is bypassing network security. Use of proxy server, VPN application or any other similar software will be counted as malpractices and in such case the account will be blocked / suspended on permanent basis.

4.3 Wireless Network

Any NAU Network service accessed through wireless device will be considered under this policy. The Wireless network services are the same as the wired network medium but accessed through wireless access point. The Wireless accessed device includes desktop computers with wifi connectivity, all in one computers, laptop/notebook computers, mobile tablets and mobile phones etc. For the wireless network access following responsibilities is given below.

4.3.1 Responsibility of IT Cell

1. The IT cell is responsible for Network connectivity up to department level.
2. The Network connectivity and the troubleshooting will be carried out by IT Cell subject to guidelines issued time by time.
3. Alteration / maintenance / extension activities in entire NAU network will be only carried out in the supervision of IT Cell.
4. IT Cell is not responsible for failure in IT devices due to electricity issues at any place.

4.3.2 Responsibility of Unit / end User

1. Department is responsible for providing power supply for the Wi-Fi Access Point.
2. The IT cell is not responsible for individual connectivity of end user's devices.
3. No end user is allowed to share their internet service account with anyone.
4. Users shall not undertake any activity through any website or applications which is bypassing network security. Use of proxy server, VPN application or any other similar software will be counted as malpractices and in such case the account will be blocked / suspended on permanent basis.

5. NAU IT Services and its Guidelines

Introduction

The NAU is offering different kinds of services to employees. The services are developed, procured, deployed, administrated and managed by the IT cell.

5.1. NAU Web Mail

NAU is offering webmail services for NAU regular staff with domain **"nau.in"**. The regular staff needs to register for the same service. Presently **"nau.in"** webmail service is hosted on Google server.

5.1.1 Role & Responsibilities of IT Cell

1. IT cell will administrate and maintain the NAU web mail services.
2. Regular staff looking to avail the **"nau.in"** webmail service shall send information to IT Cell through Head of the Unit as per issued guideline.
3. Any query regarding **"nau.in"** e-mail account shall be contacted to itcell@nau.in through head of the Unit (office) email.
4. In case a compromise of an e-mail ID is needed, the IT Cell reserves the right to reset the password of that particular e-mail ID if request comes from Unit Head login.
5. In case of a situation when a compromise of an email ID impacts a large user base or the data security of the deployment, the IT Cell shall reset the password of that email ID. This action shall be taken on an immediate basis, and the information shall be provided to the user and the unit head subsequently.

5.1.2 General Guidelines

1. All users accessing the e-mail services must use strong passwords for security of their e-mail accounts.
2. Users shall ensure that e-mails are kept confidential. Users must ensure that information regarding their password or any other personal information is not shared with anyone.
3. Auto-save of password in the Organization e-mail service shall not be permitted due to security reasons.

5.1.3 NAU Web Mail Guidelines

1. User's shall not exchange e-mails that might be categorized as harassing, obscene or threatening must be avoided.
2. Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information will be considered inappropriate.
3. Unauthorized access of the services will be considered inappropriate.This includes the distribution of e-mails anonymously, use of other officers' user IDs or using a false identity.

4. Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail will be considered inappropriate.
5. Creation and exchange of information in violation of any laws, including copyright laws will be considered inappropriate.
6. Willful transmission of an e-mail containing a computer virus will be considered inappropriate and must be avoided.
7. Misrepresentation of the identity of the sender of an e-mail will be considered inappropriate and must be avoided.
8. Use or attempt to use the accounts of others without their permission will be considered inappropriate and must be avoided.
9. Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing anti-national messages, sending e-mails with obscene material, etc will be considered inappropriate and must be avoided.
10. Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation of the account.
11. The User is responsible for any data/e-mail that is transmitted using the Organization e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.
12. Users should not share passwords.
13. In case of threat to the security, the e-mail id being used to impact the service may be suspended or deactivated immediately by the IT Cell.
14. Subsequent to deactivation, the concerned user and the Unit Head will be informed.
15. In case of retirement / death / resignation of staff from the University, Unit Head has to send the details of concerned to the IT Cell for deactivation of respective staff member email ID.

5.2. Online Examination Software

This Online examination software is a service which is technically managed by the IT Cell and functionally administered by the Registrar Office. The IT Cell is only responsible for technical support of the service.

NAVSARI AGRICULTURAL UNIVERSITY
कृषिमूला ऋद्धिः
Navsari Agricultural University
Navsari
* NAVSARI *

5.2.1 General Guidelines

1. The responsibility of the functional aspects of the Online Examination software shall be looked after by Registrar Office, Navsari Agricultural University.
2. The Technical aspects shall be the sole responsibility of IT Cell.
3. Users of this service is bound by the periodically guidelines issued by the Registrar Office and the IT Cell for using the service.
4. The decision of the Registrar Office should be final in using this service.

5.3. Online Tour Management Software

Online Tour Management software is a service helpful for the online application of tour as per the NAU statutory guidelines. The IT Cell is only responsible for technical support to users.

General Guidelines

1. The IT Cell shall carry out technical support and troubleshooting of the service.
2. Respective unit head is responsible for management of user accounts of his / her unit.
3. The users shall follow the guidelines and instructions issued by IT Cell at regular interval for the use of the service.

5.4 Online ERP service

Online ERP service deployed at NAU deals with the entire online financial services pay bill, Online GPF, Pension, Financial Accounting, Expenditure, Income and Grant services, etc.

General Guidelines

1. IT cell is responsible to carry out technical aspects of the online ERP systems.
2. Comptroller office and respective users of different units are responsible for financial aspects of the online ERP systems.
3. Registrar office and respective users of different units are responsible for administrative aspects of the online ERP systems.
4. The Users should abide by the different guidelines issued from time to time by concerned office.

6. NAU Network Monitoring and privacy Policy

The purpose of network monitoring is to identify and block malicious activity in order to protect the NAU network. In order to protect data, IT Cell may use network monitoring technologies (Firewall) to log network activity and to scan data moving across the network. These technologies may include anti-virus software, firewalls, intrusion protection and intrusion detection systems, vulnerability management systems, and database and application monitoring systems. This information may be used for identifying inappropriate use of Internet services through network.Confidentiality of all information gathered as a result of network monitoring will be maintained at all times. Access to information obtained through network monitoring will be limited to IT Cell and in the event of an investigation, shared with the due permission of Head of the University.

6.1 Network Monitoring Guidelines

1. IT Cell shall monitor user's online activities on NAU network to prevent the misuse of Internet service.
2. If end user is surfing unwanted content (pornography, movie, music, songs, games, sexist, or other such type media) then their internet account will be suspended.

6.2 Social Networking Monitoring Policy

1. Use of social networking sites by Organization is governed by "Framework and Guidelines for use of Social Media for Government Organizations" available at http://deity.gov.in.
2. User shall comply with all the applicable provisions under the IT Act 2000, while posting any data pertaining to the Organization on social networking sites.
3. User shall not post any material that is offensive, threatening, and obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
4. User shall not disclose or use any confidential information obtained in their capacity as an employee/user of the Organization.
5. Social networking websites and highly bandwidth consuming websites are strictly prohibited during office hours.

7. IT Security Policy

A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and data. IT cell reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system.

Scrutiny/Release of logs

IT Cell shall neither accept nor act on the request from any other Organization without prior permission from competent authority for scrutiny or release of logs.

8. Internet Services

8.1 Internet Registration Service

1. NAU staff members have to register for internet service account through tour management software only. Once staff has applied for registration, IT Cell will approve the same and send login id and password to the concerned staff's mobile number.
2. NAU students have to register for internet service account through NAU website only, in which they have to enter the details of enrollment number and mobile number. Once student has applied for registration, IT Cell will approve the same if student enrollment number and mobile number matches with the academic registration data and will send login id and password to the concerned student's mobile number.

NAVSARI AGRICULTURAL UNIVERSITY
कृषिमूला ऋद्धिः
Navsari Agricultural University
Navsari
* NAVSARI.*

8.2 NOC (Closure of Internet Service)

1. In case of retirement / death / resignation of staff from the University, Unit head has to send the details of concerned to the IT Cell for deactivation of respective staff member's login.
2. It is compulsory to take NOC (stop internet service) for every students before submission of thesis or completion of final examination and that too shall be taken care by respective Guide / Principal of students.
3. Those students having internet registration account have to apply for NOC through NAU website, once it is applied, IT Cell will approve the same if no misuse is done through students internet account.
4. Student which has not applied for internet registration can take NOC from IT Cell through their respective Guide or Principal.

9. Enforcement and Deactivation Policy

Enforcement

This policy is applicable to all users of Organization. It is mandatory for all users to adhere to the provisions of this policy. Organization shall be responsible for ensuring compliance with the provisions of this policy. The IT Cell shall provide necessary technical assistance to the Organizations in this regard.

Deactivation

In case of any threat to security of the Organization's systems or network from the resources and services being used by a user, the resources and services being used may be deactivated immediately by the IT cell. Subsequent to such deactivation, the concerned user and the competent authority of Organization shall be informed.

10. E-Waste

Electronic waste include desktop computer, laptop, printer, UPS, batteries, scanner, network equipment's, servers, firewall, projector, IT and Audio / Visual aid related items, etc.

General Guidelines

1. Unit / department heads are responsible to carry out e-waste as per the guidelines published by the government.
2. Unit / department heads are responsible to carry out necessary procedure for disposal of e-waste.