Regarding implementation of IT Policy-2024 in NAU.

Notification No.980/2024

It is hereby notified to all concerned that vide **Item No. 53.04** in the minutes of **53rd** Meeting of Board of Management of the Navsari Agricultural University held on **date: 01/10/2024,** Board of Management has resolved as under:

"It is hereby resolved that the Board of Management approves the IT Policy-2024 of Navsari Agricultural University, Navsari for implementation in Navsari Agricultural University for next five years." (Appendix-53.04)

IT Department, N.A.U., Navsari

Controlling Officer (IT)
Navsari Agricultural University
Navsari.

OW No. NAU/Compt/IT/**279**/2024
Navsari, Dt.17.10.2024

Copy F.W. Cs to :

1. All the members of the Board of Managements, Navsari Agricultural University, Navsari.
2. Registrar, Navsari Agricultural University, Navsari.
3. Principal and Dean of Various colleges of NAU, Navsari.
4. All the Officers of the Navsari Agricultural University, Navsari.
5. Unit/Sub-unit of NAU, Navsari.

Copy F.W. to :

1. Ps to Hon'ble Vice-Chancellor, Navsari Agricultural University.
2. Notification file of this office.

NAVSARI AGRICULTURAL UNIVERSITY

NAU IT Policy 2024

Department of Information Technology
Office of the Comptroller
Navsari Agricultural University, Navsari

Pioneered & Conceptualized by:

Hon'ble Vice Chancellor
Dr. Z. P. Patel

Edited & Published by:

Department of Information Technology
Office of the Comptroller
Navsari Agricultural University, Navsari.

Compiled by:

Dr. Timur Ahlawat
Dr. Hitesh Virdia
Mr. Chirag Naik
Dr. Vipul Shinde
Dr. Rajendra Naik
Prof. Jaimin Naik
Dr. Mahesh Desai
Dr. Bhavesh Chaudhari

Year of Publication:

October-2024

Publication number:

NAU/01/05/057/2024

Printed at :

Parth Enterprise,
Surat.

Regarding implementation of IT Policy-2024 in NAU.

Notification No.980/2024

It is hereby notified to all concerned that vide **Item No. 53.04** in the minutes of **53rd** Meeting of Board of Management of the Navsari Agricultural University held on **date: 01/10/2024,** Board of Management has resolved as under:

"It is hereby resolved that the Board of Management approves the IT Policy-2024 of Navsari Agricultural University, Navsari for implementation in Navsari Agricultural University for next five years." (Appendix-53.04)

IT Department, N.A.U., Navsari

Controlling Officer (IT)
Navsari Agricultural University
Navsari.

OW No. NAU/Compt/IT/**279**/2024
Navsari, Dt.17.10.2024

Copy F.W. Cs to :

1. All the members of the Board of Managements, Navsari Agricultural University, Navsari.
2. Registrar, Navsari Agricultural University, Navsari.
3. Principal and Dean of Various colleges of NAU, Navsari.
4. All the Officers of the Navsari Agricultural University, Navsari.
5. Unit/Sub-unit of NAU, Navsari.

Copy F.W. to :

1. Ps to Hon'ble Vice-Chancellor, Navsari Agricultural University.
2. Notification file of this office.

NAVSARI AGRICULTURAL UNIVERSITY

NAU IT POLICY 2024

NAVSARI AGRICULTURAL UNIVERSITY

-:: PREPARED BY ::-

Department of Information Technology
Office of the Comptroller
Navsari Agricultural University, Navsari.

INDEX

1. Preamble

Information Technology (IT) is a pivotal enabler of innovation, efficiency and growth in the digital age. Navsari Agricultural University, as a premier institution dedicated to agricultural research, education and extension services, recognizes the vital role IT plays in achieving its mission of sustainable agricultural development.

This **NAUIT Policy 2024** provides a comprehensive framework for the University's IT Services, management and governance of information technology resources. The policy aims to ensure that these resources are used effectively, securely and responsibly in alignment with the University's goals and the broader vision of fostering technological advancement in agriculture.

With the rapid evolution of digital tools, platforms and methodologies, this policy serves as a guiding document to promote best practices in IT governance, safeguard the University's digital assets and enhance all stakeholders' academic, research and administrative capabilities. It further emphasizes the importance of digital inclusion, data privacy and the ethical use of technology, while promoting innovation and continuous improvement in service delivery.

By adopting this policy, Navsari Agricultural University reaffirms its commitment to leveraging IT as a strategic asset for knowledge dissemination and operational excellence and contributing to the agricultural sector's growth in Gujarat and beyond.

2 Need for NAU IT Policy 2024

A structured and comprehensive IT policy at Navsari

Agricultural University (NAU) has become imperative in an era where technology drives progress. The IT Policy 2024 is essential for the following reasons:

2.1 Enhancing Academic and Research Excellence

Information technology is integral to modern education and research. A well-defined IT policy will streamline access to digital tools, databases and collaborative platforms, enhancing academic instruction quality, research innovation and knowledge dissemination.

2.2 Efficient Administration and E-Governance

An effective IT policy will help in standardizing digital systems, automate routine processes and improve operational efficiency across all departments. This will enable better E-governance, reduce manual work and enhance communication between various stakeholders.

2.3 Data Security and Privacy

As the University increasingly relies on digital platforms for storing sensitive data ranging from student records to research data, the need for robust security measures is paramount. This IT policy will establish guidelines to protect the confidentiality, integrity and availability of digital assets, ensuring compliance with national and international data protection standards.

2.4 Regulating Internet and Network Usage

With growing reliance on the internet and institutional networks, the IT policy will provide a clear framework for the responsible, ethical and efficient use of network resources. It will address bandwidth management and authorized access and ensure uninterrupted connectivity, essential for research, education, communication and extension activities.

2.5 Supporting Digital Transformation and Innovation

The policy will guide the University's digital transformation initiatives, enabling NAU to adopt emerging technologies such as artificial intelligence (AI), big data analytics, cloud computing and precision agriculture. These advancements will strengthen the University's role in leading agricultural innovation and sustainable development.

2.6 Promoting Cyber security Awareness

As cyber threats become more sophisticated, there is an urgent need to create awareness among faculty, students and staff regarding cyber security best practices. The IT policy will promote digital literacy, security protocols and proactive measures to safeguard against cyber attacks.

2.7 Compliance with Legal and Regulatory Standards

The policy will ensure that NAU adheres to relevant IT-related laws, guidelines and standards set by regulatory authorities and the government. This will help the University avoid legal liabilities anddata breaches and maintain the integrity of its digital ecosystem.

2.8 Ensuring Digital Inclusion and Accessibility

The IT Policy will emphasize the need for equitable access to technology resources for all students, faculty and staff, ensuring that IT infrastructure supports the needs of a diverse user base and promotes inclusivity.

2.9 Sustainability and Cost-Effectiveness

By providing a framework for the optimal use of IT resources, the policy will help to minimize waste, reduce costs

and ensure that investments in technology align with the University's long-term strategic goals.

3 Scope of NAU IT Policy 2024

The NAU IT Policy 2024 applies to all stakeholders of Navsari Agricultural University (NAU) and encompasses a wide range of information technology systems, services and processes. This Policy is valid for the next 5 years and can be superseded by the Government of Gujarat's Rules & Regulations, Policy and GRs over the period. This Policy can be updated during the validity period from time to time after getting approval from the Board of Management.

The scope of this policy includes:

3.1.1 Applicability to Users

The policy applies to all individuals associated with NAU, including Faculty, researchers, academic staff, Administrative, support staff, Students (undergraduate, postgraduate, doctoral and In-service candidates), Visiting scholars, external collaborators Contractual Staff (Young Professionals, Research Associates, Junior Research Fellow, Senior Research Fellow, Technical assistants and others as applicable) and any third parties or vendors who access the University's IT infrastructure.

3.1.2 IT Infrastructure and Resources

The policy governs the use, management and security of all IT resources provided by the University, including but not limited to:

- Campus and Remote Centre internet and intranet networks.
- IT Hardware Equipment used across the NAU.

- IT Software/Online Services used across the NAU.
- Hardware such as computers, servers, routers and University-owned mobile devices.
- Software applications, databases and digital tools.
- E-mail systems, cloud services and storage solutions.
- IT support services and help desk.
- IT Networking services.
- Any Other Services in the Scope of the IT hardware, Software and Online Services used in NAU.

3.1.3 Data Management and Security

This policy addresses the management, storage, sharing and protection of all types of data generated, collected and used within NAU. It covers:

- Academic data (e.g., research publications, student records, Agricultural Experiments data in AEMS etc.).
- Administrative data (e.g., HR, finance, operational data etc.).
- Confidential and sensitive data (e.g., personal data, intellectual property etc.).
- Guidelines for data backup, encryption and disaster recovery.
- As per UIDAI and Income Tax Department guidelines, AADHAR Card and PAN card Details of NAU Employees, students and users.

3.1.4 Network and Internet Usage

The policy outlines the acceptable use of university networks, including:

- Internet browsing and downloading restrictions.

- Usage of bandwidth-intensive applications.
- Access control, authentication and user privileges.
- Remote access to university networks (e.g., VPN & Remote Desktop softwares/app/ modules).

3.1.5 Cyber security

The scope includes all measures related to the prevention, detection and response to cyber security threats. It covers:

- Implementation of firewalls, antivirus software and other security systems.
- Monitoring and reporting of suspicious activities across the NAU Network.
- User responsibilities for password management, software updates and security practices.
- Incident response and recovery plans in the event of a data breach or cyber attack.

3.1.6 Compliance and Legal Framework

The policy ensures compliance with:

- IT laws, regulations and data protection standards of Government of India.
- Licensing agreements and copyright laws related to software and digital content.
- Intellectual property policies of the University related to research and innovation.
- This Policy is valid for the next 5 years and can be superseded by the Government of Gujarat's Rules & Regulations, Policy and GRs over the period.
- The user confidential data which includes but not limited to AADHAR card and PAN card must be handled as per

Rules, Regulations and Guidelines of Government, UIDAI and Income Tax Department from time to time.

The following acts of the Government of India are applicable in using the IT Resources at Navsari Agricultural University and can be superseded wherever applicable and required.

Digital Personal Data Protection Act, 2023 (DPDP Act):

This act governs the collection, processing, storage and transfer of digital personal data. It aims to balance individual privacy rights with the need to process data for lawful purposes.

Information Technology Act, 2000:

This act provides the legal framework for electronic transactions and e-commerce. It includes provisions for preventing computer-based crimes and implementing security measures.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:

These rules specify the security practices and procedures that organizations must follow to protect personal data.

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:

These rules regulate social media intermediaries and online platforms, ensuring they follow certain guidelines to protect user data and privacy.

3.1.7 Usage of Digital Communication Tools

The policy applies to the appropriate and ethical use of email, instant messaging, social media and other communication

tools provided by NAU. It includes:

- Guidelines for official use of university email accounts
- Usage of official communication channels for academic and administrative purposes

3.1.8 Procurement, Maintenance and Disposal of IT Resources

The scope covers procedures related to the procurement, maintenance and decommissioning of IT hardware and software, ensuring cost-effective and sustainable use of resources:

- Hardware and software life cycle management.
- Disposal of obsolete or retired IT equipment in an environmentally responsible manner.

3.1.9 Digital Learning and Research Platforms

The policy extends to the management and use of digital platforms that support teaching, learning and research activities:

- Guidelines for the use of online learning tools and e-resources.
- Collaboration platforms for research and academic projects.

3.1.10 Monitoring and Enforcement

The policy outlines the monitoring of IT system usage and enforcement measures for policy violations, including:

- Regular audits of network activity and system security.
- Disciplinary action in case of breaches of policy or misuse of resources.

4 IT Hardware Resource Policy

4.1 Introduction

The **IT Hardware Policy** of Navsari Agricultural University (NAU) outlines the guidelines for the **procurement**, **usage, management** and **disposal of hardware resources (E-waste) across the University**. This policy ensures the efficient, secure and sustainable use of IT hardware while supporting the institution's academic, research and administrative needs.

The IT hardware resources include desktop computers, all-in-one computers, servers, laptop/ notebook computers, thin client computers, wireless access points, Wireless adapters, network switches/hubs, printers, scanners and other computer peripheral devices, Networking devices and others as applicable for IT Equipment.

4.2 Scope of IT Hardware

The IT Department is responsible for buying and deploying the necessary IT hardware resources for providing IT services across the University. The internet connectivity services shall be procured/deployed by the IT Department subject to the budgetary provisions.

Respective units and departments are responsible for procuring and maintaining IT hardware like Desktop computers, all-in-one computers, servers, laptops/ notebooks, printers and scanners through the appropriate university-laid purchase process and Government of Gujarat Regulations from time to time.

The respective units of NAU will be fully responsible for Repair/AMC and maintenance of Hardware resources at their respective units. They are required to perform the appropriate

process in this regard as per the University's Rules and Regulations from time to time.

4.3 Usage Guideline for Efficient IT Hardware Resources

- Computers (Desktop Computers, All-In-One Computers and Laptop Computers) shall normally be used only for executing University work. Users shall exercise their own good judgment and discretion towards the use of desktop devices for personal use to the minimum extent possible.
- Users shall ensure that updated licensed antivirus/scanning software is running in the systems.
- Users shall abide by instructions, procedures/ Circulars as directed by the IT Department and competent authorities of NAU from time to time.
- The user cannot deploy/install network equipment in the university network without prior permission of the IT Department.
- Users are advised to use the Licensed operating system in the computers running at their Units.
- The users are required to ensure that all IT Hardware Equipments in their unit should have proper earthing and proper electricity supply. The IT department will not be responsible for any damage/loss due to power supply issue. In case of any damage to the IT hardware equipment due to power supply, the user department/office will be solely responsible in this regard.

4.4 Procurement of Hardware Resources

The NAU Units/Offices should prefer to purchase hardware from well-known brands through GeM Portal and as per Guidelines and purchase policy issued from the Government of Gujarat and rules and Regulations of University time to time. In addition, they should also have to consider the latest guidelines of GIL (Gujarat Informatics Limited) and DST (Department of Science and Technology) for the Purchase of IT Hardware Resources for their units.

The procurement of IT hardware must be approved by the IT Department to ensure budgetary alignment and prevent duplication of licenses.

4.5 Disposal of IT Hardware Resources

- The NAU Units/Offices are required to consider NAU E-waste Policy and Government rules and regulations from time-to-time disposal for of Hardware Resources as E-waste.
- Obsolete IT hardware will be disposed of as per e-waste management regulations to minimize environmental harm. Hardware with reusable components may be refurbished/repaired for secondary use within the University.
- Before disposal or reassignment, all data must be securely wiped/erased from devices to prevent unauthorized access to sensitive information.
- Wherever possible, obsolete but functional hardware may be donated to non-profit organizations or recycled, contributing to environmental sustainability.
- All users of IT hardware in NAU are required to comply

with this policy. Violations of the IT Hardware Policy may result incases of misuse, negligence or failure to comply with this policy, the University reserves the right to take appropriate disciplinary action, which may include suspension of hardware privilege or any actions decided by competent authorities of NAU as deemed necessary.

5 NAU IT Software Policy & Guidelines

The **IT Software Policy & Guidelines** of Navsari Agricultural University (NAU) aims to regulate the acquisition, use, management and disposal of software resources in alignment with the University's academic, research, Extension and administrative goals. This policy establishes protocols for ensuring the secure, legal and efficient use of software across all departments and stake holders. It provides guidelines for the use of software for all employees/students/contractual staff within the NAU to ensure appropriate usage. This policy applies to software obtained as part of a hardware bundle of pre-loaded software and Application Software Installed as per university requirements.

This **IT Software Policy & Guidelines** ensures that all software resources at Navsari Agricultural University are used responsibly, securely and efficiently to support the University's mission of academic and research excellence.

5.1 Procurement and Licensing of Software

To maintain compliance with legal standards and ensure optimal functionality, the University will follow standardized procedures for the procurement and licensing of software. The policy includes:

5.1.1 Software Selection:

Only authorized software that meets the University's operational, academic or research needs should be procured. The software should align with industry standards and support institutional goals.

5.1.2 Licensing Compliance:

All software must be legally licensed. The University will not tolerate pirated, unlicensed or unauthorized software. If required, The IT department will track and manage licenses to ensure compliance with software agreements.

5.1.3 Approval Process:

The procurement of software must be approved by the IT Department to ensure budgetary alignment and prevent duplication of licenses.

5.1.4 Open Source and Proprietary Software:

Where possible, the University encourages the use of open-source software to minimize costs. However, proprietary software may be procured for specialized needs that open-source solutions cannot fulfill.

5.2 Installation and Use of Software

To ensure that software resources are used effectively and securely, the following guidelines apply:

- Access to certain software may be restricted based on the roles and responsibilities of individuals within the University. Software access privileges will be managed by the IT department to ensure security and resource allocation.
- If required, The IT department will audit software installations to ensure that all software in use complies

with licensing agreements and University policy. Unauthorized software will be removed and users may face needful actions for violations.

- End users must utilize software resources only for educational, research and administrative purposes in line with the University's mission. Misuse of software for personal gain or illegal activities is strictly prohibited.
- For Special Software on University-owned device send users are advised to take the assistance of the IT Department. Faculty, staff and students are prohibited from downloading or installing software without IT approval.
- All software, especially security-related applications such as antivirus, firewalls and operating systems must be kept up to date. The IT department will monitor and implement regular patches and updates to mitigate security risks.
- Every system must have up-to-date antivirus and malware protection software installed and running to prevent unauthorized access and protect University data.
- Users must back up critical data regularly and the IT department will ensure that appropriate data recovery and backup protocols are in place for software handling sensitive or mission-critical data.
- In cases where off-the-shelf solutions do not meet the specific needs of the University, custom software may be developed or existing software customized and the IT department may develop in-house software to meet specific university needs. Such software must comply with the University's security and data management

policies.

- In cases where external vendors are hired to develop software, the University will ensure that all contracts and agreements adhere to intellectual property laws and data protection regulations.
- All new or customized software must undergo thorough testing by the IT Department before being deployed within the University's network to ensure functionality and security.
- The Software that is no longer supported by vendors or has reached to the end of its lifeshould be decommissioned after acquiring permission from competent authority.
- Before uninstalling or decommissioning software, any sensitive or valuable data must be securely archived or transferred to other platforms as per the University's data retention policies.
- Any unused or obsolete software licenses will be terminated or transferred, if possible, to optimize the University's software budget.

5.3 Compliance and Enforcement

All users of software resources within the University are required to comply with the guidelines outlined in this policy. Violations may result in:

5.3.1 Disciplinary Actions:

- Misuse, unauthorized installation or non-compliance with licensing requirements may lead to disciplinary action, including revocation of software privileges and disciplinary actions by competent University authority.

- The actions will be decided by competent authorities of NAU as deemed necessary.

5.3.2 Policy Review:

This software policy will be periodically reviewed to ensure alignment with emerging technology trends, legal standards and institutional needs.

5.4 General Guidelines to end users for software usage

- Before uninstalling or decommissioning software, any sensitive or valuable data must be securely archived or transferred to other platforms as per the University's data retention policies.
- Users shall not copy or install any software on desktop devices, including privately owned shareware and freeware, without the approval of the IT Department.
- Users shall not share their accounts, passwords, similar information or devices used for identification and authorization purposes.
- All software installation is to be carried out by the user only.
- End Users should not use any VPN and Third-party Software that exploits the firewall and makes the NAU network vulnerable to network attacks at NAU; if the user is found carrying out such malpractices, then their SSO account will be blocked/suspended permanently.
- The user is solely responsible for any user-level software issues with their computer and hardware level.
- Users shall use a strong password to defend against attacks.
- Users shall not use pirated software.

6 NAU IT Network Policy and Guidelines

The IT Network Policy of Navsari Agricultural University (NAU) is designed to ensure the secure, reliable and efficient use of network infrastructure, aligning with the university's educational, research and administrative objectives. This policy outlines responsibilities, acceptable use and security measures to maintain the integrity and performance of the network. The NAU is required to follow Telecommunication infrastructure Policy issued from Government of India time to time during the Policy validity period.

Navsari Agricultural University (NAU) Network is a Wide area network (WAN) comprised of buildings located at the Navsari campus and remote stations using IPSec VPN technology. All the IT services are delivered through this network from the NAU IT server room. NAU network can be accessed through two modes wired network (Fiber Optic based network) and wireless network. The policy for accessing wired and wireless networks is given below.

6.1 Wired Network

The wired network comprises Fiber optic cable connectivity from the server room to switches located at various buildings from there, the network is extended to switches or I/O boxes. The different roles and responsibilities for wired networks are given below.

6.1.1 Responsibility for IT Department

- IT Department is responsible for managing and monitoring of NAU wired network.
- IT Department is responsible for Network connectivity up to the main connectivity of the building only.

- IT Department will carry out the network connectivity and troubleshooting, subject to guidelines issued time to time.
- Alteration/maintenance/extension activities in the entire NAU network will only be carried out under the IT Department's supervision.
- IT Department shall not be responsible for failure in IT devices due to electricity issues, Rain, Flooding, Fire or any Natural calamity at any place.
- The IT Department will monitor and log network traffic to detect and prevent security breaches, optimize performance and ensure compliance with this policy. However, user privacy will be respected to the extent possible.
- Bandwidth usage will be prioritized for educational and research purposes. The IT department reserves the right to limit bandwidth for non-essential services during peak hours to ensure network performance.
- The IT department will schedule regular maintenance and updates to ensure network reliability and security. Where possible, these will be scheduled during off-peak hours and users will be notified in advance.
- Remote access to the university's network must be conducted using secure methods, such as Virtual Private Network (VPN) connections. Remote access is granted based on job function or educational need and users must comply with all security protocols when accessing the network remotely.

6.1.2 Responsibility of Unit / End User

- The power supply to network equipment and rack will be the sole responsibility of the respective units.
- The users are required to ensure that any IT Hardware Equipment used must have proper earthing and proper electricity supply. The IT department will not be responsible for any power supply issue. Any damages to IT hardware equipment installed by the IT Department due to power supply, The user department/office will be solely responsible in this regard.
- Unit is not allowed to make changes in the network cabling at their premise without the consent of the IT Department and such activity will be treated as network tempering.
- No end user is allowed to share their internet service account with anyone.
- Users shall not undertake any activity through any website or application bypassing network security. Use of a proxy server, VPN application or any other similar software will be considered malpractice and, in such case, the SSO account will be blocked/suspended permanently.
- Any security incidents, including unauthorized access, malware infections or network breaches, must be reported immediately to the university's IT department.
- Violation of this policy may result in disciplinary action, which could include suspension of network privileges and necessary actions decided by competent authorities of NAU depending on the severity of the violation.

6.2 Wireless Network

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

6.2.1 Responsibility of Unit / End User

- The power supply to network equipment (Wi-Fi device) and rack will be the sole responsibility of the respective units.
- The users are required to ensure that any IT Hardware Equipment used must have proper earthing and proper electricity supply. The IT department will not be responsible for any power supply issue and any damages to IT hardware equipment installed by the IT Department or Department due to power supply The user department/office will be solely responsible in this regard.
- The user is solely responsible for troubleshooting Wi-fi devices installed at their department.
- Users shall not undertake any activity through any website or application bypassing network security. Use of a proxy server, VPN application or any other similar software will be considered malpractice and, in such case, the SSO account will be blocked/suspended

permanently.

- Any security incidents, including unauthorized access, malware infections or network breaches, must be reported immediately to the university's IT department.
- Users must maintain the confidentiality of their network credentials. Passwords should be strong and users must regularly update them.
- Users must ensure that sensitive or confidential data is securely handled, stored and transmitted by university guidelines.
- Users connecting to the Wi-Fi network must adhere to the same security standards as for wired network access, including keeping devices updated and secure.
- The university's Wi-Fi network is secured using encryption. Users must ensure they connect only to authorized SSIDs (Service Set Identifiers) provided by the IT department.
- Violation of this policy may result in disciplinary action, which could include suspension of network privileges and necessary actions decided by competent authorities of NAU depending on the severity of the violation.

7 NAU Internet Service Policy & Guidelines

The Internet Service Policy of Navsari Agricultural University(NAU) is designed to ensure the responsible, secure and effective use of Internet services by the users of the university. This policy establishes guidelines for the access and use of the university's internet resources to support its academic, research and administrative objectives.

The NAU is presently using procured Internet Leased Line, NKN and GSWAN for Internet & Intranet Services. The NAU is required to follow guidelines issued from NKN **(National knowledge network)** and GSWAN **(Gujarat State Wide Area Network)**

7.1.1 Responsibility of IT Department

- The IT Department is responsible for procuring and providing Internet Services across the University.
- The Units/office are encouraged not to procure and deploy individual Internet services. If needed in special cases the IT Department's Approval is necessary in this regard.
- The IT Department is responsible for the management of Internet Leased Line connectivity for the University.
- The IT Department is not responsible for the individual connectivity of the user's devices.

7.1.2 Responsibility of Unit/end User

- No end user is allowed to share their internet service account (SSO Account) with anyone.
- The Users shall not undertake any activity through any website or application bypassing network security. Use of a proxy server, VPN application or any similar software will be considered malpractice and, in such cases, the account will be blocked/ suspended permanently.
- If any issues are experienced by users they are required to report the incident to IT Department immediately.

7.2 Access to Internet Services General Guidelines

- Internet access is provided to all registered students, faculty, staff and authorized visitors. Guests and temporary users may be granted limited internet access upon approval from the IT department.
- Users must authenticate with their assigned credentials (username and password) to access the university's internet services through NAU's SSO (Single Sign On) system. Sharing of login credentials is prohibited.
- Internet access is primarily intended for activities related to education, research and university administration.
- Personal use of the university's internet is permitted, provided it does not interfere with network performance, violate university policies or disrupt academic or work responsibilities.
- The IT department will implement firewalls, secure gateways and other security measures to protect users and university data from cyber threats.
- The IT department reserves the right to filter or block access to certain websites and online services that are deemed inappropriate or pose a threat to the network. This includes websites related to illegal activities, pornography, gambling and other non-academic content.
- All the users of the NAU's Internet Service are required to understand that the university respects the privacy of its users and monitoring may be conducted as necessary to maintain the security and integrity of the network. Any monitoring will be conducted in compliance with relevant legal and ethical standards.

- In certain cases, access to blocked sites may be granted for legitimate educational or research purposes, subject to approval by the IT department.
- Academic and research-related internet traffic will be prioritized over recreational or personal use, especially during periods of high network demand.
- The IT department may implement bandwidth caps or restrict access to bandwidth-intensive applications (e.g., video streaming and large file transfers) to ensure fair use of internet resources.
- The IT Department have reserve rights toresetlogin/ authentication credentials (password, Pin, OTP, T-OTP, QR, etc.) of the IT Services provided by NAU without any intimation for the security purpose.

7.3 End User Guidelines for using Internet Services

- Users must create strong passwords for their university accounts and update them regularly. Password sharing is not allowed.
- Users must protect confidential or sensitive data (e.g., research data, student information, financial data) and not disclose it over unsecured internet connections.
- All users must comply with this Internet Service Policy, other related university policies and applicable legal regulations. Users are responsible for their actions while accessing the internet through university resources.

The following activities are strictly prohibited in the NAU network while accessing the Internet Services

- **Illegal Activities**: Accessing, sharing or distributing content that violates local, state or national laws (e.g., piracy, hacking or unauthorized downloads).
- **Malicious Activities**: Introducing malware, viruses or attempting unauthorized access to other systems or networks.
- **Inappropriate Content**: Accessing or sharing offensive, obscene or harmful content, including hate speech, pornography or materials that harass others.
- **Commercial Use**: Using the university's internet resources for personal financial gain, commercial activities or non-university-related business ventures without proper authorization.
- **Bandwidth Abuse**: Engaging in activities that excessively consume bandwidth (e.g., large file downloads, video streaming or torrenting) that are not related to academic or research purposes.
  - Any Violations of this policy may result in disciplinary action, including the suspension of internet privileges and any other depending on the severity of the violation decided by the competent authority of the University.

7.4 Internet Registration Service Guidelines

- The Internet Registration Account of regular staff will be automatically created by the system, once details are entered in NAU's HRMS and approved by the IT Department.
- The Internet Registration Account of Adhoc staff will be automatically created by the system, once details are entered in NAU's Web management portal and approved by the IT Department.

- NAU students will get the NAU's Internet Service after Registration number is allotted.
- The notification of username created will be notified through SMS/WhatsApp/registered e-mail.
- This service may be improved from time-to time during the Policy validity period.

7.5 NOC (Closure of Internet Service) Guidelines

In case of userleft/retirement/death/resignation/ completion of study/left the study from the University, All the employees/staff/students/adhoc staff is required to generate IT Services NOC from their SSO login.It is compulsory to submit the generated NOC to the Unit Head/Principal.

7.6 Enforcement and Deactivation Policy

7.6.1 Enforcement

This policy applies to all users of IT Resources including IT Hardware, IT Software, IT Online Services and Internet Services of the University. All users must adhere to the provisions of this policy. The organization shall be responsible for ensuring compliance with the provisions of this policy. The IT Department shall provide necessary technical assistance to the Organizations in this regard.

7.6.2 Deactivation

In case of any threat to the security of the Organization's systems or network from the resources and services being used by a user, the IT Department may deactivate the resources and services being used immediately. After such deactivation, the concerned user and the competent authority of the Organization shall be informed. The IT Department is deemed to take necessary

actions as and when needed for the securing NAU IT Hardwares and Softwares.

8 NAU IT Online Services and its Guidelines

The NAU is offering different kinds of services to employees. The IT Department develops, procures, deploys, administrates and manages the services. The users are required to consider guidelines and adhere to the NAU online services.

The NAU is required to consider applicable laws and regulations for e-pay as whenever and wherever applicable for digital payments and payment gateways. The confidentiality of data is required to be followed as per guidelines issued by Government of India.

8.1 NAU Web Mail

NAU is offering web mail services for NAU regular staff and students with the domain "nau.in" and “naumail.in”. The regular staff and students need to register for the same service. Presently "nau.in" and “naumail.in” web mail service hosted on google servers.

8.1.1 Role& Responsibilities of IT Department

- IT Department will administrate and maintain the NAU web mail services.
- The nau.in based e-mail account will be created automatically once staff's detailed are entered in the HRMS. The notification of e-mail created will be notified through SMS/WhatsApp/registered e-mail.
- The NAU students can avail the NAU web mail service and apply for the same through NAU' SSO (Single Sign On) login.

- Any query regarding the "nau.in" and “naumail.in” e-mail account shall be communicated to itcell@nau.in through the head of the Unit (office) e-mail.
- The IT Department reserves right to reset login/ authentication credentials of the NAU e-mail services/account and Authentication rules/ policies provided by NAU without any intimation to user for the security purpose.
- In case of a situation when a compromise of an e-mail ID impacts a large user base or the data security of the deployment, the IT Department shall reset the password of that e-mail ID. This action shall be taken immediately and the information shall be provided to the user and the unit head.

8.1.2 General Guidelines for NAU Web mail Services

- All users accessing the NAU Web mail services must use strong passwords to secure their e-mail accounts.
- Users shall ensure that e-mails are kept confidential. Users must ensure that information regarding their password or other personal information is not shared with anyone.
- Auto-save passwords in the Organization's e-mail service shall not be permitted for security reasons.
- Users shall not exchange e-mails that might be categorized as harassing, obscene or threatening must be avoided.
- The unauthorized exchange of proprietary information or any other privileged, confidential or sensitive

information will be considered inappropriate.

- Unauthorized access to the services will be considered inappropriate. This includes anonymizing e-mails, using other officers' user IDs or using a false identity. For that necessary actions will be taken from IT Department.
- The creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mails will be inappropriate.
- The creation and exchange of information that violates any law, including copyright law and will be considered inappropriate.
- Any wilful transmission of an e-mail containing a computer virus will be considered inappropriate and must be avoided.
- Misrepresenting the sender's identification in an e-mail will be considered inappropriate and must be avoided.
- Use or attempt to use the accounts of others without their permission will be considered inappropriate and must be avoided.
- The transmission of e-mails involving language derogatory to religion, caste or ethnicity, sending personal e-mails to a broadcast list, exchanging e-mails containing anti-national messages, sending e-mails with obscene material, etc., will be considered inappropriate and must be avoided.
- Any case of inappropriate use of e-mail account shall be considered a violation of the policy and may result in the deactivation of the account.

- The user is responsible for any data e-mail transmitted using the Organization's e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.
- In case of a threat to security, the e-mail ID being used to impact the service may be suspended or deactivated immediately by the IT Department.
- After deactivation, the concerned user and the Unit Head will be informed.
- The allotted NAU web mail account of the student will be automatically deactivated after the completion of degree & notification in NAU' Exam Software.
- In special situations if student request for activation of that account, then respective NAU web mail account will be reactivated for limited time. The Decision of IT Department will be considered final to activate and deactivate the requested account.
- The IT Department will provide NAU web mail account to pensioners.
- If any regular staff leaves the University due to Resignation/Transfer to other university then their NAU web mail account will be deactivated.
- If any employees deputed to NAU then NAU web mail service account will be provided and it will be deactivated immediately after cancelation/ completion of Deputation period.

8.2 General Guidelines for NAU Online Services

- The IT Department provides various NAU online Services. All the users and stakeholders required to consider guidelines, Manuals and Instructions issued from the IT Department time to time.
- The IT Department required to develop Administrative softwares when needed as per NAU statute guidelines.
- NAU online services are available to authorized users, including students, faculty and staff through SSO (Single Sign On).
- Users are responsible for the security of their accounts and must not share login credentials with others.
- Any activity performed under a user's account is the user's responsibility, including adherence to NAU policies, legal regulations and academic integrity standards.
- The users must ensure that their devices meet the minimum-security requirements to access NAU services.
- The Users must not engage in activities that disrupt the operational NAU online services, including spamming, distribution of malware or attempts to compromise security.
- Commercial use of NAU online services without authorization is not allowed.
- The Users must follow NAU's privacy policy when handling sensitive data, including personal, academic and financial information.

- The Users should be aware of the risks associated with online communication, including potential breaches of confidentiality and take appropriate precautions.
- The Users should be aware that services may experience scheduled downtime for maintenance or updates and reasonable efforts will be made to notify users in advance.
- NAU IT Department reserves the right to monitor the use of its online services to ensure compliance with university policies and legal obligations.
- The use of online services to share or distribute copyrighted materials without permission strictly prohibited.
- Any violation of these guidelines may result in suspension or termination of access to NAU online services.
- All the users are required to understand that they are required to consider time-to-time Circulars and guidelines issued by the NAU IT Department& competent authority.

9 NAU Network Monitoring and Privacy Policy

The Network Monitoring Guidelines of Navsari Agricultural University (NAU) provide a framework for the continuous monitoring of the university's IT network to ensure its integrity, security and optimal performance. These guidelines outline the principles and procedures for monitoring network activity, safeguarding university assets and ensuring compliance

with applicable laws and policies.

The purpose of network monitoring is to identify and block malicious activity to protect the NAU network. To protect data, IT Departments may use network monitoring technologies (Firewalls) to log network activity and to scan data moving across the network. These technologies may include antivirus software, firewalls, intrusion protection and intrusion detection systems, vulnerability management systems and database and application monitoring systems. This information may be used to identify inappropriate use of Internet services through the 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 Department and in the event of an investigation, shared with the due permission of the Head of the University.

9.1 NAU Network Monitoring Guidelines

- The IT department is responsible for network monitoring and will adhere to approved standards and practices.
- IT Department shall monitor users' online activities on the NAU network to prevent the misuse of Internet service.
- The Network Monitoring will be carried out in a way that minimizes intrusion into users' privacy while maintaining the security and efficiency of the network.
- The Network Monitoring is focused on network performance and security, not individual user activities unless an investigation into policy violations or security breaches is warranted.

- The Network monitoring activity will comply with Government laws, including data protection regulations and user privacy laws as and wherever applicable.
- Real-time monitoring will be employed to alert the IT department of suspicious or unusual activities, allowing for immediate response when necessary.
- The Monitoring data will be handled with strict confidentiality and access will be limited to authorized IT personnel and administrators. Monitoring information will not be used to infringe upon personal privacy, except in cases where violations of law or policy are suspected.
- If monitoring Activity reveals a potential security breach, unauthorized access or policy violation, the competent authorities will be informed and necessary actions will be taken.
- All users are required to comply with the network monitoring guidelines and other university IT policies. Non-compliance may result in restrictions on network access, disciplinary action or legal consequences.
- Any intentional efforts to circumvent network monitoring systems, tamper with network devices or engage in unauthorized activities will be treated as serious policy violations. Violators may face disciplinary measures ranging from suspension of network privileges to legal prosecution, depending on the severity of the offense.
- The following key areas will be monitored regularly in Network Monitoring by the IT Department through the

firewall and any monitoring Mechanism

- **Bandwidth Usage**: Monitoring bandwidth consumption to identify network congestion, abuse of resources or bottlenecks.
- **Unauthorized Access**: Detecting attempts to gain unauthorized access to systems or sensitive data.
- **Network Traffic**: Analysing traffic patterns for abnormal behaviour, including large-scale downloads/uploads, Distributed Denial of Service (DDoS) attacks or malware propagation.
- **Device Activity**: Monitoring the devices connected to the network to ensure only authorized hardware is in use.
- **Security Threats**: Scanning for malware, viruses, phishing attempts or other cyber security risks.

9.2 Social Networking Monitoring Policy

- The "Framework and Guidelines govern the use of social networking sites by organizations for the use of Social Media for Government Organizations", is available at http://deity.gov.in.
- The user shall comply with all the applicable provisions under the IT Act 2000 while posting any data about the Organization on social networking sites.
- The user shall not post any offensive, threatening or obscene material that infringes copyright, is defamatory, hateful, harassing, bullying, discriminatory, racist, sexist or otherwise unlawful.
- Users shall not disclose or use any confidential information obtained in their capacity as an

employee/user of the Organization.

- Social networking websites and highly bandwidth-consuming websites are strictly prohibited during office hours.

10 NAU E-waste Policy

Navsari Agricultural University (NAU) is committed to sustainable environmental practices. This policy outlines the procedures for the responsible management of electronic waste (e-waste) generated by the university to minimize its environmental impact and ensure compliance with applicable regulations.

The E-waste disposal will be carried out as per NAU's E-waste Policyand Government Rules and Guidelines from time to time.

11 CCTV Access Guidelines

- Any NAU employee/others wishing to obtain CCTV footage from the NAU, Navsari Campus must submit a formal request through the proper channel. The request must include a recommendation from the Registrar. Without the Registrar's approval the request will not be processed.
- The CCTV Footage is subject to availability based on the retention period and storage limitations of the CCTV system. If the requested footage falls outside these parameters, it may not be available.
- The CCTV footage will be provided only if the recordings are available and meet the criteria outlined in the request.

- The request should respect privacy laws and comply with institutional data protection and confidentiality requirements.
- The request must clearly state the purpose of obtaining the footage, along with sufficient justification to ensure it aligns with NAU's policies and regulations.
- The requesting staff/others wishing to obtain the CCTV footage must consider the time-to-time guidelines issued for accessing the CCTV footage during the Policy validity period.

12 NAU Guidelines for usage of AI (Artificial Intelligence)

The following guidelines outline the responsible and effective use of Artificial Intelligence (AI) technologies at Navsari Agricultural University (NAU) to enhance agricultural research, education and extension services.

- NAU should strategically engage AI (Artificial intelligence) in the university's research, education and outreach activities to address key challenges in agriculture.
- The usage of AI in Navsari Agricultural University must adhere to data privacy laws and guidelines to protect farmers' and stakeholders' data. Data should be anonymized where necessary to safeguard personal and sensitive information.
- The University should encourage training for the usage of AI for university staff, researchers and extension officers on AI technologies, tools and their applications

in agriculture.

- The University should allocate appropriate resources, including funding, staff and infrastructure to support AI initiatives at the university.
- The University should regularly monitor and evaluate the performance of AI applications to ensure they meet the intended objectives and deliver value to agricultural Education, Research and Extension.
- The University should regularly monitor and stay updated with evolving laws and standards related to AI, data protection.
- The University must allow the usage of AI as per the Government Rules & Regulations from time to time and issue guidelines during the Policy validity period.

13 Abbreviation of Terms

NAU - Navsari Agricultural University

IT - Information Technology

AEMS - Agricultural Experiment Management System

VPN - Virtual Private Network

E-waste - Electronic Waste

AI - Artificial Intelligence

AMC - Annual Maintenance Contract

GeM - Government E-market Place

GIL - Gujarat Informatics Limited

DST - Department of Science and Technology

NKN - National Knowledge network

GSWAN - Gujarat State Wide Area Network

REMARKS & NOTES

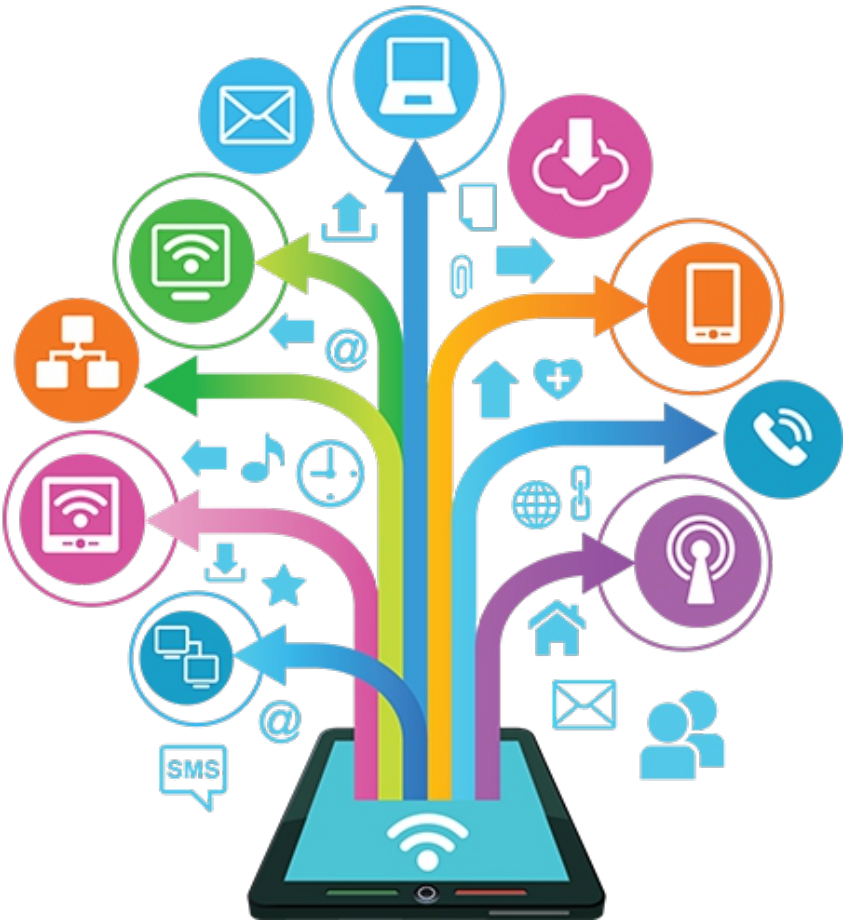
REMARKS & NOTES

REMARKS & NOTES

REMARKS & NOTES

REMARKS & NOTES

NAVSARI AGRICULTURAL UNIVERSITY



NAVSARI AGRICULTURAL UNIVERSITY

Department of Information Technology
Office of Comptroller
Navsari Agricultural University, Navsari
Pin - 396 450 (Gujarat)
Mobile : 73594 45544