Acharya Narendra Deva University of Agriculture & Technology

Kumarganj- 224 229, Ayodhya (U.P.)

IT Policy

IT POLICY

INTRODUCTION

Acharya Narendra Deva University of Agriculture & Technology (ANDUAT), Kumarganj, Ayodhya expects all individuals using ICT resources of the university to take the appropriate measures for the efficient, economical and ethical use of all the IT resource provided to create, preserve, transmit and apply knowledge through teaching, research and extension works. Computers provide unequalled opportunities to explore and use a varied and exciting set of resources. In order to make these resources available to everyone, those who use the University's available technology must do so in a way that is consistent with their educational mission. The Purpose of this policy is to present the various IT resources and services with respect to their usage, maintenance and security in order to establish the consistency in campus practice and process. This covers the use of all computers and other related hardware and the use of the network and software infrastructure. This policy document necessarily includes the Regulations and Policies applying to use of University ICT Facilities laid down by the University. In the following, the use of computers connected to the university network (main & off-campuses) both for academic and administrative purposes is covered together with the security policy and procedures.

INTERNET POLICY

Acharya Narendra Deva University of Agriculture & Technology, Kumarganj, Ayodhya provides all faculty, students, KVK scientist, research fellows and staff with a modern, fully networked computing and IT environment for academic use. Users of university 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, protect the privacy and work of students and faculty, and preserve our right to access the international networks to which the system is connected. In case of complaints, appropriate action to be taken will be decided and taken by the University Authorities.

These rules are intended to provide general guidelines to computer and Internet uses. Failure to comply with the university IT Policy rules will result to legal and disciplinary action.

Guidelines for network users

Accounts & Passwords

The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else and it will only be used for educational/official purposes. The User guarantees that the Net Access ID will always have a password. Network ID's will only be established for Students and staff who leave the University will have their Net Access ID and associated files deleted.

No User will be allowed more than one Net Access ID at a time and one login is permitted at a time, with the exception that faculty or officers, who hold more than one portfolio, are entitled to have temporary Net Access ID related to the functions of that portfolio.

Limitation on use of internet resources

The University reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

Computer Ethics & Etiquettes:

The user will not attempt to override or break the security of the University computers, networks, or machines/networks accessible there from. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages. Even sending unsolicited bulk email messages comes under IT Policy violation.

User's Net Access ID gives him/her access to email, and campus computing resources. The user of these resources must comply with University policy. The user

- should not contain copyrighted material or software unless the permission of the copyright owner has been obtained.
- should not violate University policy prohibiting sexual harassment.
- Should not be used for commercial purposes.
- Should not appear to represent the University without appropriate permission, or to represent others.

- Should not appear to represent other organizations or companies.
- Should not contain material which violates pornography laws, or algorithms or software which iftransferred violate laws.
- Should not contain scripts or code that could cause a security breach or permit use of resources inopposition to University policy.

Unauthorized access to the university wireless/Wi-Fi network using Network/RF devices by residents or employees residing nearby can lead to disciplinary action under rules against them and can lead to Fine and lodge of F.I.R. Wireless/ Wi-Fi access users need to immediately report to the university authority if any incident or suspected incidents of unauthorized access point installation are noticed.

Social Networking

All Social networking sites are barred in the campus. Accessing such site through PROXY or by using special browsers will result in the deactivation of his/her NET Access ID. Also legal and disciplinary action will be taken against the rule violator.

Account Surrendering

Retiring employees and the students leaving the university (temporarily or permanently) are advised to get their accounts (NET Access and Email) disabled by giving a written letter to university authority. This is essential as the facility is meant only for the serving employees and the enrolled students. Further, in case the accounts arenot disabled and misused by some unauthorized personals, the account holder would be legally responsible for such misuse of the account.

Account Termination and Appeal Process

Accounts on ANDUAT, Kumarganj network systems may be terminated or disabled with little or no notice. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the university authority of the same. But, if the termination of account is on the grounds of willful breach of IT policies of the University by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she should approach the university

authority, justifying why this action is not warranted.

Users should note that the University's Network Security System maintains a history of infractions, if any, for each user account. In case of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate university authorities.

INFORMATION SECURITY

The information assets of University are valuable to its objectives. The confidentiality, integrity and availability of University information assets are essential to the success of its operational and strategic activities. The University aims to secure its information assets by establishing an information security strategy that will enable the implementation of a robust information security risk management system and foster good security practices across its campuses.

The Information Security Policy is a key component of the University's Information Security Strategy built on a framework of information security management standards and best practices. The Information Security Policy will serve as an overarching policy document to provide a high level overview of information security management within the University. The following principles govern the University's information security approach:

- The University has adopted an information security risk management approach in line with the Institutional Risk Management Policy to ensure information security risk mitigation efforts reflect the University's risk appetite.
- The Information Security Policy and supplementary policies, processes, standards, procedures and guidelines has been communicated to all users via training and awareness sessions, inductions, University intranet and internet, bulletins and other appropriate communication channels.
- User access to the University's information assets will be based on job requirements rather than job titles. Access rights are reviewed at regular intervals and revoked if or where necessary.

- The University believes that information security is the responsibility of its information asset users, and will set out the responsibilities for the strategic leadership, management and coordination of the information security strategy, and use of its information assets via relevant policies, job descriptions and terms and conditions of employments.
- The University has established and promoted an information security awareness culture amongst its information asset users through user awareness and training, publications on information security risks and incidents, and guidelines for managing them.
- Disaster recovery plans for mission critical information assets and related services have been established, tested and maintained.
- The University has implemented an incident reporting and management system to enable prompt and appropriate incident resolution activities and inform risk assessments and management.
- The University enforce and monitor compliance with the Information Security Policy, supplementary policies, processes, standards, procedures and guidelines. All users of University information assets must comply with the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines and must also keep abreast of updates to these policies. Failure to adhere to the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines will be addressed by necessary disciplinary actions in accordance to the University's Staff Disciplinary Procedures, Student Disciplinary Regulations and Procedures.

NETWORK SECURITY

All users of University information assets must comply with the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines and must also keep abreast of updates to these policies. Failure to adhere to the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines will be addressed by necessary disciplinary actions in accordance to the University's Staff Disciplinary Procedures, Student Disciplinary Regulations and Procedures.

This policy applies to all members of the University community and authorized guests of the University who connect network-capable devices to the Network (wired or wireless) on campus as well as who access resources or services that are located on the Network from off campus (their home or anywhere else on the Internet).

University students, instructors, researchers and staff are authorized to connect network-capable devices of an approved type to the Network. Instructors, researchers and staff may extend this authorization to guests on a temporary basis if they judge that so doing supports the University's mission, but in so doing they assume responsibility for their behavior. Authorization and access to the Network may be withheld or withdrawn with cause.

Only approved devices and device configurations are to be connected to the Network. Information about, and configuration requirements for approved devices will be maintained and provided by university authority. Equipment that does not comply with these requirements should not be connected to the network. Exceptions to these requirements may be authorized to meet the academic needs of the University.

Any Department/Centre/Unit desiring to establish Wi-Fi at their respective departments need to take technical specification along with approved with approved configuration/make from the Directorate and devices purchased be informed and got configured from university authority in order to ensure security on Wi-Fi devices. Activities that interfere with the reliable operation of the Network are prohibited. Devices that interfere with the Network should be disconnected and/or removed.

Scanning and mapping the Network, as well as monitoring Network traffic, are prohibited unless authorized by university. The technical team of university will scan devices connected to the Network for security issues and vulnerabilities. Network traffic are monitored to help ensure a reliable Network service and to protect Network users. Devices suspected to be in violation of this policy will be disconnected from the Network. No Network/RF devices be installed anywhere in the campus without proper technical clearance /permission of the university authority, failing which disciplinary action will be taken against the defaulter and the respective equipment's will be seized

EMAIL POLICY

Electronic Mail is a tool provided by the University and serves as a primary means

of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of University Email Accounts evidences the user's agreement to be bound by this policy.

- University authority provides the email accounts to staff and research scholars.
- All staff, in particular administrative, academic and research staff should maintain and use only University email accounts and not use any external/personal account to conduct the official communications of the university.
- The University's email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments.
- University employees' e-mail addresses are not confidential. Employee e-mail addresses will be visible to other University e-mail account holders.
- E-mail sent by the University to a University e-mail account is an official form of communication to employees. It is the responsibility of employees and students to receive such communications and to respond to them as may be necessary.
- Official Communications may be time-critical and employees and students are expected to review messages sent to their University e-mail account on a reasonably frequent and consistent basis.

General Standards of Email Use: E-mail facility provided by the University should not be used:

- for the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- for the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- for activities that violate the privacy of other users.
- for the creation or transmission of anonymous messages, i.e. without clear identification of the sender.

RISK MANAGEMENT

The University's Risk Management Policy is a high level document that sets out the University's approach for managing and reducing risks to an acceptable level. In line with the Risk Management Policy, the University has developed an information security

risk management system to support faculties and administrative offices in identifying internal and external risks to the security of the University's information assets they are responsible for. Relevant, appropriate and cost effective controls along with necessary training where applicable are implemented in a timely manner to mitigate identified risks. In addition, the information security risk management system is a tool for evaluating the effectiveness of risk mitigation controls, and also informs the recommendation and implementation of new or additional controls where necessary, and ensures continuous monitoring of risks.

SOFTWARE ASSET MANAGEMENT

The University is committed to the appropriate use of Information Technology and Services in support of its teaching, research, administrative and service functions. The University's IT Acceptable Use Policy defines the acceptable behavior expected of users and intending users of the facilities, including the web facilities and systems. The University requires users to accept the IT policies and associated Requirements Governing the Use of IT Facilities as a condition of their use.

These are accessible on the University Policy Directory. These guidelines apply to all users of the university. The following general principles apply to Software Asset Management.

- It is the policy of the ANDUAT, Kumarganj University to respect all software copyrights and license agreement terms/conditions that apply to University owned software installed on University and non-University owned IT facilities, or when used directly in support of its business operations.
- IT facilities purchased with research and/or consultancy funds remain the property of the University and are treated as University owned IT facilities. Users should not duplicate any licensed software or related documentation for use either on University premises or elsewhere unless expressly authorized to do so under the prevailing software agreement.
- Users should not give licensed or copyrighted software to any external parties (including, but not limited to clients, contractors, customers), unless expressly authorized to do so under the prevailing software agreement.

- Users should use software on local area networks, licensing servers, or on multiple machines only in accordance with the prevailing software agreement.

GREEN COMPUTING

The Acharya Narendra Deva University of Agriculture & Technology, Kumarganj, Ayodhya is committed to beneficial practices towards the community and seeks to benefit many stakeholders and constituencies. As part of this, the University endeavor to do no harm and curtail impacts on the environment, locally, regionally and globally. The University seeks to manage its Information Technology resources in ways consistent with those guiding principles and our mission imperative activity in teaching, research and extension.

PURCHASING OF IT EQUIPMENTS

University has a well-defined and organized procedure for purchasing computer and IT equipments to ensure that they are equipped with the necessary technology to support the effective teaching and learning process. The following procedure can be followed:

- University allocates a budget for purchasing the required computer and IT equipments. The budget should consider the quality and quantity of equipment needed as per the indents given by the different units, as well as any additional costs such as warranties, support, and maintenance.
- University publishes national wide e-tender on etender.up.nic.in or goes to the GeM portal for purchasing the computers and IT equipments through reputable and reliable vendors who specialize in supplying IT equipment suitable for educational institutions. Consideration of factors such as vendor experience, product quality, pricing, and after-sales support. Ensure that the quotations include all relevant details such as product specifications, warranty information, and delivery timelines.
- Evaluate the technical specifications of the proposed equipment to ensure they meet the requirements of the indenters. Ensure that the equipment is capable of handling the tasks and software as per the indenter’s requirements.

- Ensure that the new IT equipment is compatible with existing infrastructure and systems at the institution. Compatibility issues can lead to unnecessary delays and disruptions in the university works.
- Prioritize the security of the IT equipment and data of the university. Implement necessary security measures to protect sensitive information and prevent unauthorized access.
- Seek necessary approvals from institutional authorities before finalizing the purchase of the computer and IT equipment.
- Issue a formal purchase order to the selected vendor based on the agreed quotation and terms. The purchase order should clearly specify the equipment details, quantities, agreed-upon price, delivery schedule, and payment terms.
- Coordinate with the vendor for the delivery and installation of the IT equipment. Ensure that the installation is carried out smoothly and that the equipment is functional.
- Conduct testing and quality assurance checks on the IT equipment to ensure they are working as expected and meeting the required performance standards.
- Maintain proper documentation of the purchased equipment, including invoices, warranties, and maintenance records. This documentation is essential for tracking equipment status and ensuring accountability.