NIIT University

IT Policies

Released on 01-April-2023

Registrar
NIIT UNIVERSITY
Neemrana

This document contains following policies:

Table of Contents

Registrar
NIIT UNIVERSITY
Neemrana

Need and applicability of IT Policy

Computers and communications Centre (CCC) maintains the policies governing the use of NU computing and IT communication resources.

The IT Policy process also includes an annual review of existing policies and a selection of those policies to be audited for verification of compliance within NU.
Every member of the NU community is bound by these policies and is expected to be thoroughly familiar with them. Violators will be subject to the full range of disciplinary sanctions, up to and including expulsion or termination. In order to retain necessary flexibility in the administration of policies, NU reserves the right to interpret, revise, or delete any of the provisions of these policies as NU deems appropriate in its discretion.

Need for IT Policy

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organization, departments and individuals who are part of NU community to understand how institution policy applies to some of the significant areas and to bring conformance with stated policies.

This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer labs, Laboratories, Offices of the Institution (e.g. admission offices outside Neemrana campus), hostels and guest houses, or residences wherever the network facility is provided by NU. Computers owned by the individuals including students, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the NU IT policy.

Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the NU IT Infrastructure, must comply with the guidelines.
Certain violations of IT policy laid down by NU by any institution member may even result in disciplinary action against the offender by the institution authorities. If the matter involves illegal action, law enforcement agencies may become involved.

Applies to

- Stake holders on campus or off campus
- Students: UG, PG, Research
- Employees (Permanent/Temporary/Contractual)
- Faculty
- Administrative Staff (Non-Technical /Technical)
- Guests

Resources

- Network Devices wired/wireless
- Internet Access
- Official Websites, Web applications
- Official Email services
- Data Storage
- Mobile / Desktop / Server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

Registrar
NIIT UNIVERSITY
Neemrana

Acceptable Use Policy

An Acceptable Use Policy is a set of rules applied by the institute, creator or administrator, academic areas, Units, internet service providers, and website owners, often to reduce the potential for legal action that may be taken by a user, and often with little prospect of enforcement.

- Employee Acceptable Use Policy
- Student Acceptable Use Policy
- Vendor Acceptable Use Policy
- Network Security Policy
- Addressing and Domain Services
- Network Connections
    - Wireless
    - External Traffic, Services and Requests
    - Network Security
    - Enforcement
    - Monitoring and Auditing
- Email Use Policy

Registrar
NIIT UNIVERSITY
Neemrana

Employee Acceptable Use Policy

Purpose

Access to computer systems and networks owned or operated by NU imposes certain responsibilities and obligations and is granted subject to institution policies. Acceptable use must be ethical, reflect academic honesty, and show restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation and harassment.

Policy Statement

1. Sharing of passwords, PINs or other authentication information is strictly prohibited. Each individual is responsible for his/her account(s), including the safeguarding of access to the account(s).

2. The use of NU resources to access, further or otherwise participate in activity which is inconsistent with the mission of the institution is prohibited. This includes, but is not limited to the following: illegal activity, sexually explicit material, hate speech, violent behaviour & bullying, spam, hacking, etc. An exemption is granted for individuals engaged in normal pedagogic related activities or research, provided that it is consistent with NU mission.

3. In addition to standard electronic resources, members of the Institution community are expected to make appropriate use of the Institution Telephone system. Examples of inappropriate actions:

    a. Unauthorized use of another individual's identification and authorization code

    b. Use of the Institution telephone system to send abusive, harassing, or obscene messages

4. The use of NU resources to conduct business for personal financial gain is prohibited.

5. Anti-virus and anti-malware software must be installed on all computers, kept up to date and currently enabled. If software is not up to date or disabled it may lead to an infection which may result in network access being disabled.

6. Although NU deploys Windows patches for Institution issued devices, all users are responsible for keeping their computer updated with all other security patches/fixes from the appropriate software update services. This includes updating applications, such as MS Office, Adobe, Firefox, Chrome, etc or any other application installed on user's device. This also includes operating system patches for non-institution devices. Computer that are not up to date, could lead to malware infection which may result in user's network access being disabled.

7. Employees are responsible for their computer, including its hardware, software, and any network traffic transmitted by it. Users are advised to contact Computers & Communication Center (CCC) if there are any questions about whether or not certain software/hardware might conflict with this acceptable use policy.

8. The use of personal routers (wireless or wired) and/or DHCP servers outside of a contained lab environment is strictly prohibited. NU will assist users in case they require additional connectivity.

Registrar
NIIT UNIVERSITY
Neemrana

9. Using the institution network to provide any service that is visible off campus without prior NU approval, is prohibited. This applies to services such as, but not limited to, HTTP (Web), SSH, FTP, IRC, email, private VPN, etc.

10. Configuring computer to provide Internet or NU network system access to anyone who is not a NU faculty, staff member or student is prohibited.

11. Connecting any device or system to the institution data networks without the prior review and approval of CCC is prohibited.

Registrar
NIIT UNIVERSITY
Neemrana

Student Acceptable Use Policy

Purpose

Access to computer systems and networks owned or operated by NU imposes certain responsibilities and obligations and is granted subject to institution policies. Acceptable use must be ethical, reflect academic honesty, and show restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation and harassment.

Policy Statement

1. Sharing of passwords or other authentication information like id cards are strictly prohibited. Each individual is responsible for his/her account(s), including the safeguarding of access to the account(s).

2. The use of NU resources to access, further or otherwise participate in activity which is inconsistent with the mission of the institution is prohibited. This includes, but is not limited to the following: illegal activity, sexually explicit material, hate speech, violent behaviour & bullying, spam, hacking, etc. An exemption is granted for individuals engaged in normal pedagogic related activities or research, provided that it is consistent with NU mission.

3. The use of NU information systems for commercial gain is prohibited.

4. Anti-virus and anti-malware software must be installed on all computers, kept up to date and currently enabled. If software is not up to date or disabled, it may lead to an infection which may result in user's network access being disabled.

5. Students are responsible for keeping their computer updated with security patches/fixes from the appropriate software update services (Windows Update on windows computers, Software Update on Apple computers). This includes updating applications, such as MS Office, Adobe, iTunes, or Firefox. Any computer that is not up to date may lead to virus infection which may result in user's network access being disabled.

6. Students are fully responsible for their computer, including its hardware, software, and any network traffic transmitted by it, regardless if this traffic was authorized by them or not. Users are advised to contact Computers & Communication Centre (CCC) for any questions about whether or not certain software/hardware might conflict with this acceptable use policy.

7. The use of personal routers (wireless or wired) and/or DHCP servers is strictly prohibited.

8. Using the institution network to provide any service that is visible off campus is prohibited. This applies to services such as, but not limited to, HTTP (Web), FTP, IRC, peer-to-peer (p2p) multimedia sharing, game servers and email.

9. Configuring computer to provide Internet or NU network system access to anyone who is not an authorized NU faculty, staff member or student is prohibited.

10. Connecting standard mobile devices used for the pursuit of academic work to NU wireless network is permitted. Connecting any other device or system to the institution data networks without the prior review and approval of CCC is prohibited.

11. Some examples of policy violations:

    a. Accessing another user's personal private data

Registrar
NIIT UNIVERSITY
Neemrana

b. Consuming a disproportionate amount of bandwidth

c. Attempting or coordinating a denial-of-service attack

d. Probing and/or exploiting security holes in other systems either on or off campus

e. Using unauthorized IP addresses

f. Using a network protocol analyser or similar mechanism without prior authorization

g. Degrading or restricting network access for others, either on or off campus

h. Connecting to Institution systems that one has not been expressly permitted to access

i. Downloading, sharing or using copyrighted material including music, movies, software or text books

j- Participating in activities which are not consistent with the Mission of the institution. In addition, network access may be disabled if NU receives complaints or otherwise detects inappropriate behaviour.

Registrar
NIIT UNIVERSITY
Neemrana

Vendor Acceptable Use Policy

Policy Statement

1. Vendor agrees to develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, security, integrity and availability of all maintained or transmitted NU data.

2. Vendor agrees to only use NU data, systems, resources, integrations, and access solely for the original purpose for which it was intended as stipulated in any contract which exists between Vendor and NU.

3. Vendor will not mine NU data for any purpose whether internal or external to Vendor Company.

4. Vendor will not share NU data with any third party, without express permission of the Institution in writing.

5. Vendor agrees to use NU data, systems, resources, integrations and access in a manner which is consistent with the Mission of the institution.

6. Vendor agrees to comply with all local laws as they apply to NU systems and data.

7. Vendor agrees to be knowable about and comply with all other NU policies.

8. The use of NU resources to access, further or otherwise participate in activity which is inconsistent with the mission of the institution is prohibited. This includes, but is not limited to the following: illegal activity, sexually explicit material, hate speech, violent behaviour & bullying, spam, hacking, etc. An exemption is granted for individuals engaged in normal pedagogic related activities or research, provided that it is consistent with NU mission.

Registrar
NIIT UNIVERSITY
Neemrana

Network Security Policy

Purpose

This policy is intended to protect the integrity of the campus network, to mitigate the risks and losses associated with security threats to computing resources and to ensure secure and reliable network access and performance for the Institution community. This policy is necessary to provide a reliable campus network to conduct and prevent unauthorized access to institutional, research or personal data. In addition, the Institution has a legal responsibility to secure its computers and networks from misuse.

Addressing and Domain Services

1. Computers & Communication Center (CCC) is solely responsible for managing any and all Internet domain names related to NU (e.g. NU.ac.in). Individuals, academic Schools/Departments or administrative departments may not create nor support additional Internet domains without prior approval from CCC.

2. To ensure the stability of network communications, CCC will solely provision and manage both the public and private IP address spaces in use by the Institution.

3. CCC may delegate administrative responsibilities to individuals for certain network ranges, but retains the right of ownership for those networks.

Network Connections

1. NU faculty, staff or students may not connect, nor contract with an outside vendor to connect, any device or system to the Institution networks without the prior review and approval of CCC. Any unit that wishes to provide Internet or other network access to individuals or networks not directly affiliated with the Institution must obtain prior approval from CCC.

2. In order to maintain reliable network connectivity, no other department may deploy wireless routers, switches, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus without prior review and approval of CCC.

3. Users are permitted to attach devices to the network provided that they are:

- for use with normal Institution or student operations
- do not interfere with other devices on the network
- are in compliance with all other NU policies.

4. Unauthorized access to Institution networking equipment (firewalls, routers, switches, etc.) is prohibited. This includes port scanning or connection attempts using applications such as SSH/SNMP, or otherwise attempting to interact with Institution network equipment.

5. Unauthorized access to Institution equipment/cabling rooms is also prohibited.

Wireless

1. Computers & Communication Center (CCC) is solely responsible for providing wireless networking services on campus. No other department may deploy wireless routers, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services on campus.

2. CCC is responsible for maintaining a secure network and will deploy appropriate security procedures to support wireless networking on campus.

Registrar
NIIT UNIVERSITY
Neemrana

3. The Institution will maintain a campus wireless network based only on IEEE 802.11 standards. CCC will collaborate with academic departments where devices used for specific educational or research applications may require specific support or solutions.

4. CCC will provide a general method for network authentication to Institution systems. The IEEE 802.1x standard is the currently supported authentication method. Additional security protocols may be applied as needed.

5. All users of wireless network resources at NU are subject to the applicable Network Acceptable Use Policy. Users of wireless resources at NU agree to have read and be bound by the terms and conditions set forth in that policy.

External Traffic, Services and Requests

1. CCC will take action to prevent spoofing of internal network addresses from the Internet. CCC will also take action to protect external Internet sites from source address forgery from devices on the Institution network.

2. The Institution external Internet firewall default practice is to deny all external Internet traffic to the Institution network unless explicitly permitted. To facilitate this, any area / unit must register systems with CCC which require access from the Internet. Users that would like to request access through the Institution firewall must discuss with CCC for this purpose.

3. Access and service restrictions may be enforced by Device, IP address, Port number or Application behaviour.

4. CCC reserves the right to decrypt SSL traffic which transits the Institution network.

Network Security

1. CCC may investigate any unauthorized access of computer networks, systems or devices. CCC will work with academic or administrative departments and law enforcement when appropriate.

2. All devices connecting to the network must have adequate security installed/maintained and must be configured and maintained in such a manner as to prohibit unauthorized access or misuse.

3. If a security issue is observed by any user (Faculty/Staff/student/guest), it is the responsibility of all NU users to report the issue to the appropriate supervisor or CCC for investigation.

4. CCC reserves the right to quarantine or disconnect any system or device from the Institution network at any time.

5. Network usage judged appropriate by the Institution is permitted. Some activities deemed inappropriate include, but are not limited to:

Attaching unauthorized network devices, including but not limited to wireless routers, gateways DHCP or DNS servers; or a computer set up to act like such a device.

a. Engaging in network packet sniffing or snooping.
b. Setting up a system to appear like another authorized system on the network (Trojan).
c. Other unauthorized or prohibited use under this or any other Institution policy.
    i. Students may consult the Student Acceptable Use Policy for further information.

Registrar
NIIT UNIVERSITY
Neemrana

ii. Employees may consult the Employee Acceptable Use Policy for further information.

Enforcement

1. Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network or systems connected to it, is subject to immediate disconnection from the Institution network. CCC may subsequently require specific security improvements where potential security problems are identified before the device may be reconnected.

2. Attempting to circumvent security or administrative access controls for information resources is a violation of this policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of this policy.

3. The Institution reserves the right to test and monitor security, and to copy or examine files and information resident on institution systems related to any alleged security incident or policy violation.

Monitoring and Auditing

1. CCC will maintain and monitor traffic logs for all network devices and systems for security auditing purposes.

2. CCC reserves the right to monitor, access, retrieve, read and/or disclose data communications when there is reasonable cause to suspect a Institution policy violation, criminal activity, monitoring required by law enforcement or with appropriate management request. Reasonable cause may be provided by the complaint of a policy violation or crime or as incidentally noticed while carrying out the normal duties of CCC staff.

3. CCC may perform penetration testing of any Institution owned devices or systems on its networks in order to determine the risks associated with protecting Institution information assets. CCC may further perform non-intrusive security audits of any system or device attached to the Institution's networks in order to determine what risks that system may pose to overall information security.

Registrar
NIIT UNIVERSITY
Neemrana

E-mail policy

Conditions of use

1. All Users (faculty, Staff and Students) will have an e-mail account provided by NU. The e-mail system will provide a single externally accessible e-mail address for users. The address will not contain the name of internal systems or groups.

2. Appropriate and reasonable use of the e-mail facilities is defined as use that is consistent with objectives of the University and with the specific objectives of the project or role for which such use was authorized. Electronic mail and communications facilities provided by NU are intended for official communication. Limited personal use is acceptable if it does not hurt the interests of the University. NU reserves the right to limit, restricts or extends access to them.

3. All persons using the e-mail facilities shall be responsible for the appropriate use of the facilities provided as specified in the "Responsibilities" and "Code of Practice" sections of this document. Administrators at sites may provide additional guidelines.

4. The University recognizes the need to protect the confidentiality of information and material furnished by Employee and all users should protect the confidentiality of such information and material. The University takes safeguard measures to protect information from losses within the University's e-mail facilities. The user must also take all reasonable measures to further safeguard against any loss of information within the University's e-mail facilities under his/her control.

5. Users of the e-mail facilities recognize that when they cease to be formally associated with the University (e.g. no longer an employee or completion of training), their information may be removed from University's e-mail systems without notice.

6. The University reserves the right to limit permanently or restrict any user's usage of the e-mail facilities with or without notice to the user in order to protect the integrity of the e-mail facilities against unauthorized or improper use, and to protect other users.

7. The University, through authorized individuals, reserves the right to periodically check and monitor and take any action to protect e-mail facilities from misuse.

An action will be deemed as misuse if the user is:

- Responsible for willful physical damage to any of the e-mail facilities.
- In possession of confidential information obtained improperly.
- Responsible for willful destruction of information.
- Responsible for deliberate interruption of normal services provided by the e-mail facilities
- Gaining or attempting to gain unauthorized access to accounts and passwords.
- Gaining or attempting to gain access to restricted areas without the permission of the administrator.

RESPONSIBILITIES

Registrar
NIIT UNIVERSITY
Neemrana

Electronic mail can be both informal like a phone call and yet irrevocable like an official memorandum. Because of this, users should explicitly recognize their responsibility for the content, dissemination, and management of the messages they send. This responsibility means ensuring that messages:

- Do not contain information that is harmful to the University or staff of the University.
- Are courteous and polite.
- Are consistent with University's policies; and are not used for purposes that conflict with University's interests.
- Protect others' right to privacy and confidentiality.
- Do not contain obscene, offensive, or slanderous material.
- Contain an accurate, appropriate, and informative signature; Signature should not contain yahoo or Hotmail or ID from any other ISP; Home phone numbers should not be a part of the signature.
- Do not unnecessarily or frivolously overload the e-mail system (e.g. spamming, junk mail and use for entertainment is not allowed).
- Do on subscribe to list servers for entertainment. Limited subscription is permitted, if relevant for your role without adding undue load or cost to the system. Do not provide your e-mail to friend, who may indulge in similar communication.
- Downloading Attachments and circulating them over Official facility is unacceptable.
- Starting or participating in chain mails is unacceptable.
- Users will unsubscribe and inform people who are likely to send them mails, when leaving NIIT UNIVERSITY.
- Do not send VBS, EXEs etc., which are prone to virus infection.
- Sending huge attachments may choke facilities, causing delay to important communication.

Users should access their mails regularly and acknowledge mails received by them, whenever required. Large files as e-mail attachments should be avoided to the extent possible.

It is a good practice not to open e-mails from unknown users or unexpected attachments.

Users should cover periods of absence by adopting an appropriate functional authorization, forward, or out of office message strategy.

Electronic mail containing a formal approval, authorization, delegation or handing over of responsibility with clients, must be copied to paper and filed appropriately for purposes of evidence and accountability.

Users must ensure that personal and University information in their custody is protected. They constitute University's Intellectual Property or profile and can be misused by recipient(s).

Space limit on mail account

- All students, faculty and staff are provided the NU email account <your-emailid> @st.niituniversity.in on Google workspace.
- As per the policy, following space limit will be implemented in the account:
    - Faculty members: 50 GB
    - Non-academic staff: 25 GB
    - Current enrolled students: 25 GB.
    - Graduated students:
        - Students who have paid lifetime Alumni fee : 20 GB for life.
        - Other students
            - 20 GB for up to 2 years after graduation

Registrar
NIIT UNIVERSITY
Neemrana

- 5 GB after 2 years.
- This limit includes the space used by account for email + Google drive + photos.
- All users should review the files in the account and use the space responsibly.
- If any additional space is required by **faculty** for any official project/requirement, then the limit for faculty can be increased to 75GB or max 100 GB on recommendation from area directors.
- The limit for **non-academic staff** can be increased to 50GB on recommendation from unit head.
- If any **students** need additional space for their projects, then they should contact the respective faculty/project mentor. The faculty member can create a shared folder in their account and provide access to that student/team.
- When a user reaches the space limit in the account, they will see the relevant warning on login to the account, and the system will not allow user to add further files or edit existing files. Users are requested to please take a backup of files and photos in some other location and maintain the space used in the NU account within the specified limit.

CODE OF USE

- Use of UNIVERSITY e-mail to participate in chain letters is not acceptable.
- The use of e-mail in any way to facilitate the conduct of a private commercial purpose, gains, free offers, or schemes is forbidden.
- If the UNIVERSITY provides access to electronic mail to external users such as consultants, temporary employees, or partners, they must read and adhere to Standards and Guidelines for use of e-mail. The usage must be strictly for services to NIIT UNIVERSITY.
- Confidential or University proprietary information will not be sent by e-mail. Users found to be deliberately misusing e-mail will be dealt with as per HR policies.
- All electronic messages created and stored on UNIVERSITY computers or networks are property of the UNIVERSITY and are not considered private.
- Users must not allow anyone else to send e-mail using their accounts. This includes their supervisors, secretaries, assistants, and any other subordinates.

- Encryption shall be used for any information classified sensitive or confidential that will be transmitted over open networks such as the Internet.
- Incoming messages will be scanned for viruses and other malign content.
- As University's networks and computers are the property of the University, NU retains the right to allow authorized UNIVERSITY staff to monitor and examine the information stored within.
- It is recommended that personal confidential material not be stored on or sent through NIIT UNIVERSITY's equipment.
- Users must ensure the integrity of their password and abide by guidelines on password security (see the relevant section on password security).
- Sensitive confidential material should be sent through the electronic mail system after encryption or password protection.
- Confidential information should be redirected only where there is a need and with the permission of the originator, where possible.
- Users should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies.

Registrar
NIIT UNIVERSITY
Neemrana

Electronic mail messages can be forged in the same way as faxes and memoranda. If a message is suspect, users should verify its authenticity through other communication channels. Do not reply to suspect e-mails.

Registrar
NIIT UNIVERSITY
Neemrana

Hardware and Software Procurement Policy

Policy

1. The procurement of all computing and communication hardware and software is coordinated by the office of Computers & Communication Center (CCC) in order to maximize the NU investment in Information Technology (IT).

2. To take advantage of IT tools in the most cost-effective manner possible, the NU has standardized a series of hardware and software products that integrate easily with the Institution's IT infrastructure. An up-to-date list of supported hardware and software js available from CCC. When considering the purchase of hardware or software, all aeas and units should coordinate their purchase with CCC.

3. While the acquisition of standard products is encouraged, some areas / units have need for special equipment or software not included in the list of supported products. CCC will consult with the department to select the most appropriate equipment and to work out an agreement for continued support.

4. Departments who choose to buy IT resources not approved by CCC are responsible for their implementation and ongoing maintenance. CCC will not be responsible for interfacing such hardware or software to the campus network or information repository.

5. In accordance with the NU funding philosophy, costs for the acquisition of IT resources are borne by the purchaser area/unit.

Registrar
NIIT UNIVERSITY
Neemrana

Password Management Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of a department's entire network. Any device connected to the campus networks must implement authentication and authorization processes that uniquely identify all users and appropriately control access to systems.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all faculty, staff and students who have or are responsible for an account (or any form of access that supports or requires a password) on any system connected to the campus network, has access to the campus network, or stores any non-public NU information. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

Policy:

NU requires that:

- All systems-level passwords (e.g., root, administrator, network administrator, application administration accounts, etc.) must be changed at least every 180 days.
- All production system-level passwords must be part of the Team password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused the past 10 passwords.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

Users must select strong passwords. Strong passwords have the following characteristics:

- Be at least 12 - 32 characters in length
- Be a mixture of letters and numbers
- Be changed at least every 90 days
- Be different from the previous 10 passwords
- Can NOT contain your EMPID, First Name, or Last Name
- Not contain 4 consecutive characters used from the previous password
- Not contain the user's user id
- Note that poor, weak passwords have the following characteristics:
- The password contains less than six characters _\')\K
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, and so on
    - Computer terms and names, commands, sites, companies, hardware, software

Registrar
NIIT UNIVERSITY
Neemrana

- Birthdays and other personal information such as addresses and phone numbers
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, and so on
- Any of the above spelled backwards

* Any of the above preceded or followed by a digit (for example, secret1, 1secret) Further, systems that authenticate must require passwords of users and must block access to accounts if more than three unsuccessful attempts are made.

Members of the NU must follow these guidelines for passwords:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an e-mail message
- Don't talk about a password in front of others
- Don't hint at the format of a password, like, "my family name"
- Don'treveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers

Members of NU must not use the "Remember Password" feature of applications.

Members of NU must not write passwords down and store them anywhere in your office. Further, passwords must not be stored on ANY computer system without encryption.

Registrar
NIIT UNIVERSITY
Neemrana

Social Media Policy

With the rise of social media as a communication platform, the way in which User (Faculty, Staff and Student) of NIIT University communicate internally, externally as well as online, continues to evolve. While this creates new opportunities for communication and collaboration, it also creates larger responsibilities for the Users.

Guidelines to be followed by Faculty, Staff and Student

1.1. It is the responsibility of Faculty, Staff and students to:

1.1.1. to read and act in accordance with these guidelines, and any additional guidelines published by NU to read and act in accordance with the rules and guidelines set out by individual Social Media, Social Networking and Website Hosting companies and providers

1.1.2. to Consult with your project guide and where relevant seek ethical approval before posting, as part of your studies / research, pictures, videos, or comments through social media that could be viewed as offensive or as bringing NU into disrepute.

1.2. The Faculty, Staff and Student shall:

1.2.1. not use the social media for raising and escalating concerns relating to his/her course, NU or any members of NU. He/she must lodge a complaint at the URL https://nucleus.niituniversity.in/ in complaint menu, or directly give it to relevant authority (e.g. Dean student affairs or Dean Academics office).

1.2.2. Ensure not to reveal confidential information about NU or its staff, students, partner organizations or clients.

1.2.3. Not violate the relevant professional codes when using social media as part a research study or project.

1.2.4. Ensure not to use any site or pages in any way that may compromise your current or future fitness to practice or employability.

1.2.5. Not use NU's logo or brand without obtaining permission of Marketing team of NU (Marketing@niituniversity.in

1.2.6. Consult Marketing team of NU (Marketing@niituniversity.in if there is any media interest resulting from your online activity.

1.3. The Faculty, Staff and Student must beware that:

1.3.1. that third parties including the media, employers and Police can access profiles and view personal information. This includes pictures, videos, comments, and posters. Inappropriate material found by third parties affects the perception of the student and NU and can have a negative impact on a student's prospects.

1.3.2. Communications made in a personal capacity including posting images or links to content through social media must not:

A. be unlawful – i.e. breach any applicable criminal and/or civil laws of India,

B. include anything that could be considered discriminatory against, or bullying or harassment of, any individual. This includes:

I. making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age

II. using social media to bully another individual or

III. posting images that are discriminatory/offensive or links to such content

IV. include defamatory comments about individuals or other groups.

Registrar
NIIT UNIVERSITY
Neemrana

C. bring disrepute to NU. This includes:

I. Pictures, videos, or comments that are of a sexual nature including links to websites of a pornographic nature and other inappropriate material

II. Pictures, videos, or comments that promote or encourage drunkenness or drug-related activity. This includes but is not limited to images that portray the personal use of drugs and drug paraphernalia.

III. Pictures, videos, or comments that depict or encourage unacceptable, violent, illegal or dangerous activities e.g. sexual harassment or assault, fighting, vandalism, academic dishonesty, drunkenness, drug use etc

IV. breach copyright ex. using someone else's images or content without permission; failing to give acknowledgement where permission has been given to reproduce something.

V. breach confidentiality ex. revealing confidential information owned by NU, giving away confidential information about an individual or organization.

VI. use NU's logo on personal social media sites.

Non-Compliance

Non-compliance with this policy may result in any or all of the following:

7.1. Limitation or revocation of individual's or group's rights to use or participate in NU related social media.

7.2. Removal of posts or social media accounts; or

7.3. Corrective or disciplinary actions and sanctions including rustication, dismissal, or termination, as the case be, as per the applicable Policies of NU.

Registrar
NIIT UNIVERSITY
Neemrana

NU Responsible Bug Disclosure Policy

All of us understand the importance of data security in today's world. We also realize that securing our system against threats of illegal data access, data corruption, etc requires intensive and ongoing efforts.

While the NU IT team does their best at their end to ensure safety and security of our systems and data, we understand that there may be some security issues unknown to us.

Therefore, we want to involve the NU students and staff in our attempts to ensure data security on all our systems, and invite you to report any such issues to the NU technology team. Any such people will be suitably recognized and rewarded within the defined framework given below:

1. Various critical IT systems holding sensitive data for the university include:
   NU digital platform, NU Academic ERP NUcleus, Learning Management System Moodle, Gatepass system, Library management system Koha, NU Cashless payment methods, Financial ERP NAV, NU Website, NU internal servers in the data center and network, NU domain directory, and NU WiFi network and internet access.
2. All security issues reported by students or staff will be categorized as follows:
   a. **Category A:** Highest category, where it is possible for an unauthorized person to access ***and*** modify/delete/corrupt NU's academic or financial data. It might also be allowing an unauthorized person to login and impersonate another authorized user, to access/modify data or content.
   b. **Category B**: Medium category, where it is possible for an unauthorized person to access and/or view any sensitive data like academic records, personal records, financial records, etc.
   c. **Category C**: Low category, where the above two conditions are not met but a security breach is possible in some other way.
3. In normal circumstances, if an NU staff or student is found to be in the knowledge of any security vulnerability and willfully conceals it from NU authority and/or disseminates this information to others, they can be prosecuted with appropriate disciplinary/legal action.
4. If an NU staff or student voluntarily reports any such security breach issue to NU authority and ensures confidentiality of such issue, then the person reporting the issue will be recognized and rewarded under this program. This will apply to CCC staff, but not including those applications which are directly developed/maintained by that staff.
5. **Any such security breach issue should be reported in a weblink, which will be shared in mail by IT team to all students.** These reported errors will be accessed by
   - Director, IT services: Akhlesh Agarwal (Akhlesh.agarwal@niituniversity.in)
   - IT head: Puneet Bajpai (Puneet.bajpai@niituniversity.in).
6. The following details should be reported for each bug:
   i. NU System and where the bug was found, and the specific URL.
   ii. Category of the issue (as recognized by you).
   iii. Description of the bug, along with steps to replicate it (if possible).
   iv. Possible resolution of the bug (optional: If known to user).
   v. Relevant screenshots, if applicable.
   vi. Any other information or attachment as applicable.
   vii. Person details (Enrollment no., name, batch, phone no. of student submitting it). If the issue is reported by staff, then please provide your employee code, name, phone number etc.

Registrar
NIIT UNIVERSITY
Neemrana

viii. A declaration stating that the lapse has not been used by person to advantage of himself/herself.

7. Link to a form, where students can submit the bug information will be sent to students via mail.
8. NU IT team will verify the security issue thereafter, and send another confirmation to the sender of the issue. NU IT team will then take required steps to ensure that the security issue is resolved on an urgent basis.
9. For each security issue reported and confirmed by NU IT manager, the person reporting the issue will get following points:
   a. Category A: 10 points
   b. Category B: 5 points
   c. Category C: 2 points.
10. Students who collect maximum points through the year will be rewarded as per the following guidelines:
    a. 1st position: ₹ 20,000
    b. 2nd Position: ₹ 10,000
    c. 3rd Position: ₹ 5,000
11. Students are entitled for award certificates and cash award as per this policy. Staff members will get only recognition certificates.
12. In case the same issue is reported by more than one person, the person who reported the issue first will get credit for the same.
13. NU IT Manager will decide the correct category (A, B or C) for each issue reported. In case of any disagreement with the sender of the issue, this will be reviewed by the IT Director. The decision of the IT director in this regard will be considered final and cannot be contested by the reportee.
14. All students/staff who report a valid bug will be given a certificate by NU in recognition of their contribution. Student contribution in this regard will also be counted in points for Ram-Rajindra medal.
15. These awards and recognition certificates will be given away during the Annual Award Function, along with other certificates for sports and co-curricular activities. On mail, a confirmation for the same will be given immediately after verification of the issue by NU IT team.
16. The person reporting the bug must maintain confidentiality and should not disclose the vulnerability with other students or faculty, and/or anybody outside NU. Any such disclosures will be considered a willful breach of security, and disciplinary/legal action can be taken against those persons.
17. The person reporting the bug should not store screenshots or other details of the issue on any external websites like Imgur, Vimeo, YouTube, Dropbox, etc.
18. While performing the research, there should not be any disruption of systems, privacy violations and/or degradation to user experience.
19. DDoS attacks DO NOT qualify under this program, and NU systems should not be tested against such attacks.

Registrar
NIIT UNIVERSITY
Neemrana

Data Privacy Policy

1. Introduction

At NIIT University, we are committed to protecting the privacy and confidentiality of all data entrusted to us, including student data. This Data Privacy Policy outlines the guidelines and best practices for staff and faculty to ensure the responsible handling and protection of sensitive data.

2. Scope

This policy applies to all staff and faculty members of NU who handle or have access to sensitive data, including but not limited to student records, financial information, research data, and any other personally identifiable information (PII) related to students, employees, or other individuals.

3. Responsibilities

3.1 Data Custodianship: All staff and faculty are responsible for safeguarding the data they handle and ensuring compliance with this policy.

3.2 Data Access: Access to sensitive data should be granted only to authorized individuals who require it to perform their job duties.

3.3 Data Security: Staff and faculty must implement appropriate security measures to protect data from unauthorized access, including the use of password protection and encryption where applicable.

3.4 Data Sharing: Sensitive data, especially student data, should not be shared via unsecured channels such as email. Instead, utilize secure, password-protected file sharing platforms approved by the university.

3.5 Data Disposal: When data is no longer needed, it should be securely disposed of according to university guidelines and applicable laws and regulations.

4. Guidelines and Best Practices

4.1 Email Communication: Avoid sending sensitive data, such as student records or personally identifiable information, via email. If necessary, use encrypted email services or secure file attachments.

4.2 Password Protection: Use strong, unique passwords for accessing university systems and databases. Passwords should not be shared with others and should be regularly updated.

4.3 Data Encryption: When storing or transmitting sensitive data, ensure that it is encrypted to prevent unauthorized access. Use encryption protocols approved by the university's IT department.

4.4 File Sharing: Utilize university-approved file sharing platforms that provide secure, password-protected access to shared documents. Avoid sharing sensitive data through public or unsecured file sharing services.

Registrar
NIIT UNIVERSITY
Neemrana

4.5 Data Minimization: Only collect and retain the minimum amount of data necessary to fulfill your job duties. Regularly review and delete any unnecessary data to reduce the risk of data breaches.

4.6 Training and Awareness: Provide regular training and awareness programs for staff and faculty on data privacy best practices, including the importance of protecting sensitive data and the consequences of non-compliance.

5. Compliance and Enforcement

Violation of this Data Privacy Policy may result in disciplinary action, up to and including termination of employment. Staff and faculty members are expected to report any suspected violations of this policy to the appropriate university authorities.

6. Review and Revision

This Data Privacy Policy will be reviewed periodically to ensure its effectiveness and compliance with relevant laws and regulations. Any updates or revisions to the policy will be communicated to all staff and faculty members in a timely manner.

7. Contact Information

For questions or concerns regarding this Data Privacy Policy, please contact the NU Computer and communication Office .

By adhering to the guidelines outlined in this policy, staff and faculty members play a crucial role in upholding the privacy and security of sensitive data at NIIT University.

Registrar
NIIT UNIVERSITY
Neemrana

Backup Policy

Policy Statement

This policy is committed to describing the Planning and Execution of Backup of Relevant Data for the NIIT University ("NU") to ensure Accessibility of live data and services by reducing downtime. NU is committed to provide security of data during storage and backup in their database with strong and recent encryption technique.

Purpose

This policy sets out obligations of NU, regarding safety, backup and retention of Personal information & Sensitive personal information (PI & SPI), it collects, stores or processes.

Scope

This policy is applicable to the backup of critical information of Students, Employees & Vendors for NU. This also includes backup of all systems and applications including (Academic ERP, Finance ERP, Website, Exam system, Gatepass, Library system, Newsletter etc).

Backup Schedule, Location & responsibility

System	Differential backup	Full backup	Transactional backup	Backup location	Responsibility
Academic ERP	Daily (except Sunday)	weekly (Sunday)	every 30 Min.	on Azure	NIIT: JD & Team
Finance ERP	every 15 min.	Daily		on the local server and on NAS	CCC: Puneet
Website		Daily		on Azure storage	CCC: Puneet
Exam system		Daily		on azure storage	CCC: Puneet
Gatepass		Daily		on the local server	CCC: Puneet
Library Koha		Twice a week (Tuesday & Friday)		on the local server	CCC: Puneet
Learn portal		Daily		on cloud	NIIT: Dewan & team

Review Schedule Of Policy

Annually by the CCC Office

Backup log

- Backup log is available on the sharepoint folder: https://niitu.sharepoint.com/:f:/s/BackupReport/EicFEtJB__JFoVA-VLC8A5EB-1ucBrk-VXHt0JIEOBpJ0w?e=7QKUe7

Registrar
NIIT UNIVERSITY
Neemrana

Information Technology (IT) Asset Lifecycle Policy

1. Introduction

This IT Lifecycle Policy outlines the procedures and guidelines for the management of IT assets throughout their lifecycle at NIIT UNIVERSITY. The purpose of this policy is to ensure the efficient and effective utilization of IT resources, compliance with regulatory requirements, and the maintenance of security standards.

2. Scope

This policy applies to all IT assets owned by NIIT UNIVERSITY, including but not limited to hardware, software, networking equipment, and peripherals.

3. Definitions

- **IT Asset:** Any hardware, software, or component used to enable, support, or deliver IT services.
- **Lifecycle:** The stages through which an IT asset passes from acquisition to disposal.
- **Acquisition:** The process of procuring new IT assets.
- **Deployment:** The installation and configuration of IT assets for operational use.
- **Maintenance & Upgrade:** The ongoing management, support, and updates of IT assets.
- **Disposal:** The retirement or decommissioning of IT assets at the end of their useful life.

4. Responsibilities

- **Computer and Communication Center (CCC):** The CCC is responsible for developing and implementing procedures for the acquisition, deployment, maintenance, and disposal of IT assets.
- **Asset Owners:** Department heads or designated personnel are responsible for overseeing the lifecycle of IT assets within their respective areas, including the submission of requests for new acquisitions and the notification of asset disposal.
- **Users:** All employees are responsible for using IT assets in accordance with organizational policies and reporting any issues or concerns to the IT department.

Registrar
NIIT UNIVERSITY
Neemrana

5. Lifecycle Stages

5.1. Acquisition

- All requests for new IT assets must be submitted to the CCC with approval from President / Vice President.
- The CCC will evaluate requests based on needs, budget, and compatibility with existing infrastructure.
- Approved acquisitions will be procured through authorized vendors and included/updated in the IT asset inventory.

5.2. Deployment

- Upon receipt of new IT assets, the CCC will be responsible for installing, configuring, and testing the equipment or software.

5.3. Maintenance and upgrade

- The CCC will establish a schedule for routine maintenance activities, including software updates, security patches, and hardware inspections of laptops, desktops issued to employees.
- IT assets issued to laboratories will come under laboratory assistant purview and he shall be responsible for maintaining and upkeep of such assets.
- Users should promptly report any issues or malfunctions with IT assets to the CCC for resolution through compliant management.
- In case of PCs, Laptops and servers, RAM, SSD etc can be added for upgrading assets. CCC team in consultation with users of the asset will look at the possibility and utility of upgrading assets. Assets will be upgraded if it will result in continued satisfactory use, and it is economically feasible.
- In some cases, the old or lower configuration asset may be useful for some specific requirements. Then they may be moved to another laboratory. E.g. moving PCs from programming lab to some labs with less computationally intensive requirements.

5.4. Disposal

- CCC will evaluate fitment and continued usage of all assets in discussion with users. IT assets that have reached the end of their useful life or not amenable for repairs or are no longer required at the current location will be processed for disposal / decommissioning as required.
- Disposal methods may include recycling, donation, or secure destruction to prevent unauthorized access to sensitive data.

6. Compliance

Registrar
NIIT UNIVERSITY
Neemrana

- All IT asset management activities must comply with relevant laws, regulations, and industry standards.
- Regular audits may be conducted to ensure compliance with this policy and identify areas for improvement.

7. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment, as well as legal consequences for non-compliance with regulatory requirements.

8. Review and Revision

This IT Lifecycle Policy will be reviewed annually and updated as necessary to reflect changes in technology, organizational requirements, or regulatory standards.

9. Approval

This policy has been reviewed and approved by

Registrar
NIIT UNIVERSITY
Neemrana