NAVRACHANA UNIVERSITY
a UGC recognized University

Information Technology

The Navrachana University Information Technology (IT) Policy sets forth the central policies that govern the responsible usage of all users of the University's information technology resources. This comprises the IT facilities allocated centrally or by individual departments. Every member of the University is expected to be familiar with and adhere to this policy. Users of the campus network and computer resources ("users") are responsible to properly use and protect information resources and to respect the rights of others.

NUV endeavours to provide all faculty, students and staff with a modern, fully networked computing and IT environment for academic use.

Users of NUV 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 person in-charge of the facility in consultation with the Registrar/Provost as appropriate.

Introduction

1.1. NUV provides IT resources to its employees to enhance their efficiency and productivity. These resources are meant as tools to access and process information related to their areas of work. These resources help NUV staff/faculty to remain well informed and carry out their functions in an efficient and effective manner.

1.2. For the purpose of this policy, the term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

1.3. Misuse of these resources can result in unwanted risk and liabilities for the NUV. It is, therefore, expected that these resources are used primarily for NUV related purposes and in a lawful and ethical way.

Applicability

The IT Policy applies to all University faculty, staff and students and all others using the IT resources, whether personally or of University owned, which access, transmit or store various types of related information.

1. Objectives

Each user of the University Information Resources must ensure that it is used for promoting the mission of the University towards teaching, learning, research, and administration. In particular, the major objectives of this document are:

1.1 To ensure the integrity, reliability, availability, and superior performance of the University IT Systems

1.2 To ensure that the IT resources protects the official e-identity (allocated by the University) of an individual

1.3 To ensure that all the users of the University are responsible for adhering to the procedures governing the implementation of this Policy document and any other matter incidental to those rules

2. Areas

2.1 IT usage and Prohibitions

2.1.1 The users of the University shall make effective usage of campus systems, internet, wireless resources, official websites (including university website, conference website, journal portals, online admission systems, and course website), and ERP solutions, Learning Management System, Remote Login based facilities of the University and e-Library resources.

2.1.1 The University shall stress upon the users to comply with University policies and legal obligations (including licenses and contracts).

2.1.2 The University shall strive to arrange for awareness programs to acquaint the users with the effective usage of IT resources.

2.1.3 Prohibited Use - The users shall not send, view or download fraudulent, harassing, obscene, threatening, or other messages or material that are a violation of applicable law or University policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.

2.1.4 Copyrights and Licenses - Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file?sharing using the University's information resources is a violation of this policy.

2.1.5 Social Media - Users must abide by the rules of the University towards the usage of social networking sites, mailing lists, news rooms, chat rooms and blogs.

2.1.6 Commercial Use - The University IT resources shall not be used for any commercial and promotional purposes, through advertisements, solicitations or any other message passing medium, except as permitted under University rules.

2.1.7 Faculty, staff, and students with authorized accounts may use the computing and IT facilities for academic purposes, official work, and for limited personal purposes so long as such use

2.1.8 does not violate any law, Institute policy or IT Act 2008 of the Government of India.

2.1.9 does not interfere with the performance of Institute duties or work of an academic nature (as judged by the NUV Registrar/Provost).

2.1.10 Users are expected to respect the privacy of other users and they may not allow any other person to use their password or share their account. It is the users' responsibility to protect their account from unauthorized use by changing passwords periodically and using passwords that are not easily guessed. Sharing of passwords for any purpose whatsoever is strictly prohibited. Users may share the required files through a sharing software with proper Access Control List.

2.1.11 Any attempt to circumvent system security, guess others passwords, or in any way gain unauthorized access to local or network resources is forbidden. Users may not use another person's computing account, attempt to forge an account identity or use a false account or e-mail address.

2.1.12 Transferring copyrighted materials to or from the NUV systems without the express consent of the owner is a violation of international law. In addition, use of the internet for commercial gain or profit is not allowed from an educational site. If done so, it will be the sole responsibility of the user.

2.1.13 Downloading and installing of new software has to be done with the explicit consent of the respective facility in-charges. Installation of unlicensed software on NUV facilities, or on individual machines connected to the NUV network, is strictly prohibited.

2.1.14 Setting up of any facility requiring password transmission over clear text is prohibited without TLS/SSL encryption.

2.1.15 To the extent possible, users are expected to use only their official email addresses provided by NUV for official communications with other members of the Institute.

2.1.16 It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. It is also forbidden to send emails or messages masquerading as another person or to hide the sender's identity. Chain (Anonymous origin) letters are not allowed. Neither is any form of commercial advertising or soliciting allowed. Spamming is strictly disallowed. Subscribing to mailing lists outside the Institute is an individual's responsibility. Subscribing someone else to any group outside NUV is illegal.

2.1.17 To the extent possible, users are expected to connect only to the official NUV Wi-Fi network for wireless access. Setting up of unsecured Wi-Fi systems on the NUV network is prohibited.

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

2.1.19 Display of offensive material (either on computer screens or through posters etc.) is strictly disallowed and serious action will be taken against offenders.

2.1.20 Violations of policy will be treated as academic misconduct, misdemeanour, or indiscipline as appropriate. Depending upon the nature of the violation, the institute authorities may take an action by issuing a warning through disabling the account. In extreme cases, the account may be completely deleted and/ or the user prohibited access to IT facilities at NUV, and/ or sent to the Institute disciplinary action committee as constituted by the Institute authorities.

2.1.21 The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through the newsgroups.

2.2 Security and Integrity

2.2.1 Personal Use - The University IT resources should not be used for activities violating the basic functionality and mission of the University, except in a purely incidental manner.

2.2.2 The users must refrain from making any unauthorized access of information in order to promote secure access of Network and Computers.

2.2.3 The competent system administrator may access the information resources for a legitimate purpose.

2.2.4 Firewall - Additional procedures to maintain a secured flow of internet and intranet based traffic in the campus shall be managed through the use of Unified Threat management (firewall).

2.2.5 Anti-virus and security updates - The regular updating of the anti-virus policy and security updates should be done for the protection of computing resources.

2.3 IT Asset Management

2.3.1 Asset Management: The University shall lay down business processes for the management of hardware and software assets that facilitates the usage of IT resources in the University. This shall include procedures for managing the purchase, deployment, maintenance, utilization, energy audit, and disposal of software and hardware applications within the University.

2.3.2 Copying and Distribution: The University shall ensure that there is no violation in the copying and distribution of proprietary and licensed software.

2.3.3 Risks: The University shall emphasize on managing the risks involved for the usage of IT resources. This shall include standard procedures for identification, minimization and monitoring of risk impact by preventive and corrective measures. This should also include procedures for timely data backup, replication and restoring policies, power backups, audit policies, alternate internet connectivity for a fail-safe internet access.

2.3.4 Open Source Asset: The University shall endeavor towards the promotion and effective usage of open source software.

3. Operating Aspects:

3.1 University Governance - The University shall endeavor to ensure fair implementation of this policy so as to meet with the objectives of its formation. The responsibility of the management of operational aspects of IT resources vest with the Registrar's office.

3.2 The respective Heads of the Institutions shall be responsible for compliance with all University policies relating to the use/ownership of information resources, keeping in mind the Vision and Mission of the University.

3.3 The Head - IT working at University Level shall coordinate various activities related to the adherence of the IT Policy in association with the IT Administrator of the respective Institute.

3.4 Individual Users - The users are solely responsible for the activities they perform on Institute/University servers with their "User Name/Password" pairs and IP (Internet Protocol) addresses assigned to them.

4. Violation of Policy

Any violation of the basic objectives and areas mentioned under the IT Policy of the University shall be considered as a violation and as a misconduct and gross misconduct under University Rules.

5. Implementation of Policy

For implementation of this policy, the University will decide necessary rules from time to time.

6. Review and Monitoring

The Policy document needs to be reviewed at least once in two years and updated if required, so as to meet the pace of the advancements in the IT related development in the industry.

Review of this policy document shall be done by a committee chaired by the Registrar of the University. The other members of the committee shall comprise of the Dean of School, program Chairs, Head of Schools, Head - IT and other members as nominated by the Chair.

DECLARATION / UNDERTAKING FROM THE FACULTY / STAFF

1. I, Mr. /Ms....., Programme....., School ....., faculty/staff of Navrachana University, Vadodara (NUV), permanent resident of .... Mobile: ....., do hereby undertake on this the..... (Day), of..... (Month) ..... (Year), the following: -
2. I, hereby, declare that, the entries made by me in the Declaration/Undertaking are complete and true to the best of my knowledge and based on records.
3. [Content] I shall be responsible for all use of this network. In case I own a computer / laptop / tablet / mobile and decide to connect it to NUV, network, I will be responsible for all the content on it, especially that which I make available to other users. In case I do not own a computer but am provided some IT resources by NUV, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on Computer Centre or Department machines).
4. [Licensed Software] I will be held responsible for using Un-Authorised (Pirated) Software, Operating System on my personal computer, laptop, any device that is connected to NUV network. I fully understand the Indian Software Piracy Act stated as "Under the Indian Copyright Act, a software pirate can be tried under both civil and criminal law. The minimum jail term for software copyright infringement is seven days, and the maximum jail term is three years. Statutory fines range from a minimum of 50,000 to a maximum of 200,000 rupees."
5. [Network] I will be held responsible for all the network traffic generated by "my device". I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipment's, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerade for anyone else.
6. [Academic Use] I understand that the IT infrastructure at NUV is for academic use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law. I shall not use Institute Logo on the social sites without prior permission from competent authority. Further, I shall not air my grievances on the social sites/media till I exhaust all remedies available in the Institute for redressal.
7. [Identity] I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use NUV IT resources to threaten, intimidate, or harass others.
8. [Privacy] I will not intrude on privacy of anyone. In particular, I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.
9. [Monitoring] I understand that the IT resources provided to me are subject to monitoring, with cause, as determined through consultation with the NUV administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize NUV administration to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of NUV network.
10. [Viruses] I shall maintain my computer on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, Trojans, and other similar programs.

11. [File Sharing] I shall not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material).
12. [Security] I understand that I will not take any steps that endanger the security of the NUV network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the NUV campus. In critical situations, NUV authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of NUV.
13. [Penalties] I understand that any use of IT infrastructure at NUV that constitutes a violation of NUV Regulations could result in administrative or disciplinary procedures. If I violate any of the above or any other act which is against interest of Institute/Society at large, I shall be liable for any major or minor penalty as deemed fit by the competent authority.

Date: Signature Faculty/Staff

DECLARATION / UNDERTAKING FROM THE STUDENT

1. I, Mr. /Ms....., Programme....., School ....., Enrolment ID ..... Student of Navrachana University, Vadodara (NUV), permanent resident of .... Mobile: ....., do hereby undertake on this the..... (Day), of..... (Month) ..... (Year), the following:
2. I, hereby, declare that, the entries made by me in the Declaration/Undertaking are complete and true to the best of my knowledge and based on records.
3. [Content] I shall be responsible for all use of this network. In case I own a computer / laptop / tablet / mobile and decide to connect it to NUV, network, I will be responsible for all the content on it, especially that which I make available to other users. In case I do not own a computer but am provided some IT resources by NUV, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on Computer Centre or Department machines).
4. [Licensed Software] I will be held responsible for using Un-Authorised (Pirated) Software, Operating System on my personal computer, laptop, any device that is connected to NUV network. I fully understand the Indian Software Piracy Act stated as *"Under the Indian Copyright Act, a software pirate can be tried under both civil and criminal law. The minimum jail term for software copyright infringement is seven days, and the maximum jail term is three years. Statutory fines range from a minimum of 50,000 to a maximum of 200,000 rupees."*
5. [Network] I will be held responsible for all the network traffic generated by "my device". I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipment's, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerade for anyone else.
6. [Academic Use] I understand that the IT infrastructure at NUV is for academic use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law. I shall not use Institute Logo on the social sites without prior permission from competent authority. Further, I shall not air my grievances on the social sites/media till I exhaust all remedies available in the Institute for redressal.
7. [Identity] I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use NUV IT resources to threaten, intimidate, or harass others.
8. [Privacy] I will not intrude on privacy of anyone. In particular, I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.
9. [Monitoring] I understand that the IT resources provided to me are subject to monitoring, with cause, as determined through consultation with the NUV administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize NUV administration to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of NUV network.
10. [Viruses] I shall maintain my computer on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, Trojans, and other similar programs.
11. [File Sharing] I shall not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material).

12. [Security] I understand that I will not take any steps that endanger the security of the NUV network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the NUV campus. In critical situations, NUV authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of NUV.
13. [Penalties] I understand that any use of IT infrastructure at NUV that constitutes a violation of NUV Regulations could result in administrative or disciplinary procedures. If I violate any of the above or any other act which is against interest of Institute/Society at large, I shall be liable for any major or minor penalty as deemed fit by the competent authority.

Date: Signature Student

Internet Facility Usage Indemnity Agreement

FACILITY USAGE PERIOD _____

FACILITY USER _____

1. I hereby agree and accept that I am bound by the terms of this agreement for usage of internet provided to me by the University.
2. I state that by accessing the Internet, I may be deemed to have accepted the terms and conditions contained in this Internet Access Indemnity Agreement and shall be bound thereby.
3. The access of the internet services refers the usage of University network and any hardware and software services provided by the University. The internet access is solely for academic use by students of the University and hence should not be used for any other purpose than legal and academic use that may be in conflict with the role of the user/student.
4. The University Internet access does not permit any communication of information using the internet access of the University that may harm, threaten, intimidate, or harass others, or may be otherwise considered objectionable or illegal as per law.
5. The student hereby declares and states that he / she will not download any pirated, illegal, pornographic, violent and or morally repudiable content using the internet of the University.
6. Users are solely responsible for all and any data stored or sent by them using the internet access of the University. Any liability arising out of any misuse is the responsibility of the user/student concerned.
7. The user is solely responsible for opening any mail or attachment or downloading or installing from websites that is from unknown and suspicious sources, or is of otherwise suspicious nature without confirming the authenticity of the attachment.
8. With this, users are solely responsible for understanding and following the usage policy of the internet access. Any violation of any part of this usage policy and/or misuse of any part of the internet access by any user/ student or using any account owned by the user is solely the responsibility of the user. Any liability or legal action arising out of any such violation/ misuse will solely be the responsibility of the user, and the user will be subjected to appropriate actions as deemed fit.
9. I hereby also indemnify the University from all actions including monetary damages that they may have to face for any usage of the internet by me.

I agree to the above

Name _____

Registration No. _____

Cell No. _____

SOCIAL MEDIA

Non Negotiables, if any of the following are found to be exercised, published, encouraged, NUV will be liable to take stern action in terms of rusticating student, suspension/termination of NUV employee and in worst scenario lodge/file police complain/legal action.

In general, you should avoid posting the following:

1. Post Illegal Activities That means drugs, violence, or any sort of stealing or damaging of property!
2. Bullying towards peers, class mates, NUV students, faculty/staff.
3. Share sexually explicit stuff...you know what we're talking about. That can come back to haunt you in the long run.
4. Do not speak poorly about Peers/Faculty/Staff
5. Post Objectionable Content from NUV Computers or Networks
6. Posting of NUV Confidential Information
7. Lie / Cheat / Plagiarize
8. Threaten / Violence
9. Ignore NUV-Specific Policies
10. Unprofessional Public Profiles
11. Negative comments, posts or messages
12. Questionable or compromising photos of yourself OR others
13. Offensive jokes, photos or material
14. Overt bragging
15. Highly emotional content, like rants about personal situations or relationships

Remember, once you post something online, it's there forever. In short, be aware of what you post on your social media or networking profiles because what goes around, comes around.

DATA - BACKUP POLICY

The main goals of data backup are

- To define and apply a clear backup and restore standard for all NUV information systems.
- To define backup and recovery standards as per data prioritization.
- To prevent the loss of data in the case of accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes when such events occur.
- To manage secure backup and restoration processes and the media employed in the process.
- To set the retention periods of information contained within system-level backups designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.

NUV - Data Backup System

- where backups are located - Presently on premises, we need to have off the site backup copy
- who can access backups and how they can be contacted - backups are accessed by ICT technician, ICT head
- how often data should be backed up - everyday morning 2 a.m. to 5 a.m. backup for important data is scheduled
  - important data is categorised as
  - Active Directory - Main Server
  - All Virtual Machines
  - Important Mail Accounts
  - LMS System Data
- what kind of backups are performed - Incremental Backup is performed
  - An incremental backup copies only the data that changed since the last backup operation. This means that a smaller amount of data is being copied per system, so the backups complete much faster. Incremental backups are known to take longer to restore, as the restore uses that last full backup created plus the incremental backups captured.
- what hardware and software are recommended for performing backups - NUV has installed Q-NAPP with Veeam Backup & Replication is Software & QNAPP is the hardware backup

IT/ICT Purchase Policy

The purpose of the IT Procurement policy is to ensure that the procurement of information technology hardware, software and services follow established Navrachana University, Vadodara policies and guidelines, that due diligence is performed to ensure compatibility with existing systems and policies, that appropriate plans are associated with technology acquisition and that the approval of the Provost/Registrar is obtained prior to issuance of a purchase order.

IT Hardware & Software Procurement Guidelines

- Information Technology is the sole authority for purchasing IT hardware, software, and services for the University. These include laptops, desktops, tablets, phones, mobile devices, printers, storage, servers, and cloud services.
- A department or individual must purchase computer hardware and software through IT. Hardware or software not purchased through IT may not be eligible for reimbursement.
- Items purchased using any university funds including individual grants, remain property of the University and not the individual or department.
- At a minimum all equipment must be tagged as an asset for inventory and tracking purposes.

IT's Commitment to the Process

- Providing consulting services including designing the optimal specifications which meet the individual or department requirements.
- Obtaining the best price and/or service.
- Prompt delivery and installation of equipment and software.
- Installing University licensed software.
- Providing access to University assets including the Internet, networked drives and printers, wireless and wired networking

Guidelines

- The IT Department is the sole authority for submitting requisitions for IT hardware, software, and services on behalf of any School/Program/Dept. that has had approval for obtaining such hardware, software, and services.
- All IT related hardware, software and services will be specified by the Registrar/Head of IT. Hardware, software and services cannot be purchased without a completed IT Procurement Authorization Form. This needs to be completed and signed by the user's Coordinator/HOD/Program Chairs/Dean;
- On receipt of the completed form, IT will acknowledge receipt and the form will be processed;
- The Registrar/Head of IT will make a decision whether to approve, decline or amend the requirements for the purchase of the equipment;
- If hardware, software, and services is declined or changed, the Registrar/Head of IT will provide a brief explanation to the requesting user for the decision;
- If the hardware, software, and services is approved or changed then IT will order the hardware, software, and services directly with supplies;
- Hardware, software, and services will only be ordered according to IT work load, and the hardware, software, and services /users priority within this work load. Where equipment is Authorised and ordered, an installation window will be proposed, however this may change according to IT priorities;

- Hardware, software, and services suppliers are also recommended by the IT Department but may be changed, in agreement with the Registrar/Head of IT, by the Supplies Department in favour of a better price or service.;
- The IT Department will request that equipment be delivered to the IT Department. Here it can be checked for damage and compliance with the ordered specification before being set up and transported to its final destination.;
- The IT Department will be responsible for arranging delivery of the equipment from the IT Department to its intended destination;
- The IT Department will inform the original requestor of the equipment when the equipment is delivered to the IT Department, and will make arrangements for installation;
- The IT Department has a standard set-up procedure for new hardware, software and systems. This procedure ensures the equipment is configured correctly and that all IT security measures are addressed. This includes the setup of passwords, anti-virus software and security marking the equipment;
- The IT Department will not install software or hardware unless it has been involved in the specification of both. Hardware and software cannot be installed by staff;

Quotations/Inquiry

- For each requirement inquiry will be raised by procurement/purchase department based on approval, terms & conditions, specifications and quantity from IT department.
- Minimum three quotations are required for any IT purchase
- If the requirement approx. value is less than 1 lac, quotations can be received through mail (purchase@nuv.ac.in). Mail will be opened by Registrar along with 3 personnel of purchase body/indenting School/Program
- If the requirement is above 1 lac, sealed quotations will be a must and will be opened by Registrar along with 3 personnel of purchase body/indenting School/Program

INDENT FOR PURCHASE OF NEW ITEM **NAVRACHANA UNIVERSITY**

Indenter/Department : I.C.T **Date** _____

Item	N - New R- Replacement A - Additional	Qty	Present Stock Level & Working Condition of the Item indented	Suggested Supplier, Specification, Approx. Value, Remarks

Indenter **Authorised By (Registrar)**

Date **Date**

Password Policy

Policy Statement

All individuals are responsible for safeguarding their system access login and mail password credentials and must comply with the password parameters and standards identified in this policy. Passwords must meet the complexity requirements outlined and must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

Reason for Policy

Assigning unique user logins and requiring password protection is one of the primary safeguards employed to restrict access to the Navrachana University, Vadodara network and the data stored within it to only authorized users. If a password is compromised, access to information systems can be obtained by an unauthorized individual, either inadvertently or maliciously.

Individuals with NUV wide ID are responsible for safeguarding against unauthorized access to their account, and as such, must conform to this policy in order to ensure passwords are kept confidential and are designed to be complex and difficult to breach. The parameters in this policy are designed to comply with legal and regulatory standards.

1. Individual Responsibilities

Individuals are responsible for keeping passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:

- NUV passwords must be changed immediately upon issuance for the first-use.
- NUV passwords must never be shared with another individual for any reason or in any manner not consistent with this policy. A shared or compromised NUV Wide ID password is a reportable ICT security incident.
- NUV Wide ID passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats on untagged (unsupported) devices. Passwords should not be stored in a web browser's password manager on an untagged device.
- Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.

2. Responsibilities of Systems Processing Passwords

All NUV systems-including servers, applications, and websites that are hosted by or for NUV-must be designed to accept passwords and transmit them with proper safeguards.

- Passwords must be prohibited from being displayed when entered.
- Passwords must never be stored in clear, readable format (encryption must always be used).
- Passwords must never be stored as part of a login script, program, or automated process.
- Systems storing or providing access to confidential data or remote access to the internal network should be secured with multifactor authentication.
- Encrypted password hashes must never be accessible to unauthorized individuals.
- Where possible, salted hashes should be used for password encryption. Exceptions should be filed and reviewed on a regular basis.
- Where any of the above items are not supported, appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized individuals have access to readable passwords.

3. Password Requirements

The following parameters indicate the minimum requirements for passwords for all individual accounts where passwords are:

- At least eight (8) characters;
- Not based on anything somebody else could easily guess or obtain using person related information (e.g., names, NUV Wide ID, telephone numbers, dates of birth, etc.);
- Not vulnerable to a dictionary attack (see Recommendations for Creating Compliant Passwords section); and,
- A combination of at least one character from each of the following four listed character types
  - English uppercase letters (A-Z),
  - English lowercase letters (a-z)
  - Base 10 digits (0-9)
  - Non-alphanumeric (such as ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . / and space)

4. Password Expiration

In order to prevent an attacker from making use of a password that may have been discovered, passwords are deemed temporary and must be changed regularly. ICT Security reserves the right to reset a user's password in the event a compromise is suspected or reported. The required frequency at which passwords must be changed every six (6) months

5. Mobile Devices

Mobile devices accessing or storing NUV data, such as smartphones and tablets, shall be tagged and managed by the Firewall platform (Binding of MAC Address).

6. Recommendations for Creating Compliant Passwords

In order to create a password that is compliant with the parameters specified in this policy, use one of the three methods below.

6.1 Use a Passphrase

6.2 Use an Acronym

6.3 Use a Secret Code

File naming best practices

- Files should be named consistently
- File names should be short but descriptive (<25 characters)
- Avoid special characters or spaces in a file name
- Use capitals and underscores instead of periods or spaces or slashes
- Use date format ISO 8601: YYYYMMDD
- Include a version number
- Write down naming convention in data management plan

Elements to consider using in a naming convention are

- Date of creation (putting the date in the front will facilitate computer aided date sorting)
- Short Description
- Work
- Location
- Project name or number
- Sample
- Analysis
- Version number