KIBOGORA INSTITUTE A.K.A.

”KIBOGORA POLYTECHNIC”

ICT POLICY

Introduction:

The main purpose of this policy is to demonstrate the function of information security of networked single use (NSU). Information security is a critical component that is required to enable and ensure the availability, integrity and confidentiality of data, network and processing resources required for the NSUs to perform its business and operational practices.

1. HARDWARE SECURITY

The H variable has sub variables such that we can choose one depend of your situation you are.

a. Unattended NSU Equipment, Clear Desk and Clear Screen

- All sensitive documents and storage media containing sensitive documents will be locked away when not required and especially when the office is vacated.
- All computer screens will be set to lock automatically after 5 minutes of inactivity.
- All computer screens will be locked when left unattended.
- All NSUs are responsible for implementing security procedures for protecting unattended equipment's.
- All NSUs shall terminate active sessions by using Ctr+Alt+Del and then enter when there is a need to step away from the system.
- Sensitive or critical business information, e.g.: on paper or on electronic storage media, should be locked away (ideally in a safe or specialized cabinet or other forms of security furniture) when not required, especially outside the normal working hours.
- Computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password when unattended and should be protected by key locks, passwords or other controls when not in use.
- Incoming and Outgoing mail point and unattended machines should be protected\
- Unauthorized use of photocopiers and other reproduction technology like scanners, digital cameras, should be prevented.
- The documents containing sensitive or classified information should be removed from printers immediately.

2. PHYSICAL SECURITY

The objective is to prevent unauthorized access, damage and interference to business premises and information. It is essential that critical information processing facilities are housed in secure areas, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference, commensurate with the identified risks. The practices of "clear desk" and "clear screen" should be encouraged to reduce the risk of unauthorized opportunist access to facilities.

A good investment is a security cable with a lock for securing your laptop at a workstation or any other location that requires such. They're relatively inexpensive and a great deterrent to any thief.

a. **Use strong passwords.** When turning on your laptop, your initial password should be extremely strong, with a combination of letters, numbers, and symbols used. Once your initial password is compromised, the contents of your entire laptop (especially if you're not using full-disk encryption) can be compromised. Don't use terms and phrases for which somebody might find an association with you, such as favorite football team, home address, middle name, etc.

Password construction

NSUs should choose passwords that are easy to remember but difficult to guess. Some of the guidelines for password constructions are:

- Quality password with sufficient minimum length eight characters long
- Easy to remember
- Not based on anything, somebody else could easily guess or obtain using persons related information (e.g.: Names, Telephone Number's, Date of Birth, NSU, Spouse Name etc.)
- Not vulnerable to dictionary attack (i.e. do not consists of words included in dictionaries)
- Free of consecutive identical, all-numeric or all alphabetic characters
- Do not use word or number patterns like aaabbb, qwerty, zyxwvuts,123321, etc
- Not use the same password for business and non-business purposes
- Strong password must have at least 8 characters, at least 1 digit(s), at least 1 lower case letter(s), at least 1 upper case letter(s), at least 1 non-alphanumeric character(s)

- ❖ One way to create complex but easy to remember passwords is to take a known word or passphrase and convert it using numerals, special characters and capital letters. For example, the passphrase/word might be “moodle” and password could be: “M00dle!!”

b. It’s your laptop. Therefore, don’t let other individuals use it, especially if it’s somebody you don’t know. When situations arise that require it to be used by someone other than you, create a guest account for their use.

c. Keep a watchful eye. Don’t ever leave your laptop unattended in any public venue or location not considered safe. That means not using the coffee house phrase “can you watch my laptop for a minute as I go to the restroom”, or any other similar thought process. Being vigilant and watchful at all times is a must for the safety and security of your laptop, so remember “do not leave it unattended” plain and simple. If you have to leave in your hotel room or some other location, then remove it from sight and place under a pillow, in a closet, or some other location. The best safety measure is to carry it with you at all times.

d. Place your contact information somewhere visible. Because most people are honest and Reliable, should your laptop be stolen, misplaced or lost “and then subsequently found by a Good Samaritan” you’ll clearly want your name, phone number, address, and/or email visible on it. Put a sticker on the cover or back of your laptop with all your relevant contact information.

e. And if your laptop is stolen. Laptops unfortunately do get stolen, so think and act quickly, which means reporting the theft to local authorities along with informing management (and the I.T. department) immediately.

f. Environmental Security

- The backup files and sensitive paper of NSU will be kept securely off-site. The backups will be stored in appropriate environmental conditions as per the manufacturers' specifications taking into account air conditioning, humidity etc.
- Fire detection and suppression systems will be installed to safeguard NSU assets against fire and tested once every year.
- Firefighting mock drill / Power outage mock drill will be conducted at least once in a year
- NSU will ensure that the security personnel and personnel often working in the secure area are trained in using fire extinguisher equipment.
- Environmental conditions like humidity, pests etc. will be considered while securely sitting / storing the IT equipment, paper of NSU, backup tapes etc.
- The power supply equipment, air-conditioning and other equipment will be protected from disruptions, power surges. All such equipment will be under annual maintenance contracts with service level agreements. Records will be kept for all suspected or actual faults, and all preventive and corrective maintenance.
- Cabling (Power and telecommunication) carrying data or supporting information services should be properly labeled (point to point) with necessary identification methods and protected from interception or damage.
- power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;
- A NSU patch list should be used to reduce the possibility of errors
- A service assets register shall be maintained to record the maintenance activities carried out for critical equipment like UPS, ACs etc.
- All critical equipment will be adequately insured.

g. Physical Security Perimeter

- Security perimeter for the office premises, stock of their personnel devices and other sensitive business areas will be defined to form a physical boundary.
- Different areas of the NSU will be categorized under following classifications:
    - Fist Zone- Areas accessible to public e.g. Reception
    - Second Zone- Areas not accessible to public but accessible to all friends

- Third Zone- Secure Areas.

- Third Zone will have motion sensors or CCTV camera implemented to detect any unauthorized movement. All entrances / exits to Third Zone areas and Second Zone areas, all Fist Zone areas will be monitored though closed circuit television (CCTV) systems.
- Third Zone will have a two factor authentication system over and above proximity card access control system.
- Fire doors and emergency doors will be alarmed, monitored and tested every quarter
- All the critical or sensitive information processing facilities shall be housed in secure areas
- An entry / exit log for all the visitors entering Second Zone and Third Zone areas will be maintained.
- External party personnel entry to Third Zone areas will be allowed only after prior authorization by the ISO.
- Visitors to Third Zone areas will be escorted throughout their stay.
- Visitors will be asked to declare their belongings at entry and this will be verified when the visitors exit.
- A separate list of external party personnel who require long term access will be maintained
- All personnel entering Second Zone or Third Zone areas will be required to wear a visible identification.
- All NSU are required to wear an Identification
- A list of personnel having access to Third Zone areas will be maintained. Access rights to Third Zone areas will be reviewed on a quarterly basis.
- All delivery will be received in Fist Zone areas. If access to Second Zone or Third Zone areas is required, the delivery personnel will be escorted throughout their stay.
- Photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed in red zone, unless authorized by the ISO.

i. Data security

a. Access of Documentation

- The NSU will ensure that all documentation is handled as per its classification.
- Access to documentation shall be approved by NSU to prevent possible data loss and logs of all such approvals should be maintained.
- Process owners shall ensure that their documentation are stored securely to avoid possible misuse or disclosure from unauthorized NSUs.

b. Password Use

1) NSU will not keep copy of password in any written form or electronic form. If absolutely required, passwords of critical NSU accounts shall be maintained securely.
2) NSUs will change passwords whenever there is any indication of possible system or password compromise.
3) NSUs will change Passwords at regular intervals 90 days or based on the number of access (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid reusing or cycling old passwords.
4) NSUs will change temporary passwords at first logon
5) NSUs must not include password in any automated logon process, e.g.: stored in a macro or function key
6) NSUs will not share their passwords with anyone.
7) NSUs will ensure that nobody is watching when the password is being entered
8) The NSU before to connect to the wireless access points he/she can check if is secured with help of a security key.

c. Protection of NSU records

- The NSU shall identify and document all records that need to be maintained to meet statutory, regulatory, contractual and business requirements.
- The NSU shall also identify the retention period for the records.
- The NSU shall ensure that appropriate protection measures are taken to protect the Confidentiality, Integrity and availability of the records.

d. Prevention of misuse of information processing facilities

- The IT Team shall ensure that all NSUs are presented with a login banner at the time of accessing an IT System.
- The HR Department shall ensure that all NSUs are made aware of their responsibilities towards the proper use of information processing facilities.
- The IT Team/Admin Department shall ensure that appropriate detection mechanisms are implemented to ensure the proper use of IT facilities.
- All NSUs shall need to take prior approval from their reporting manager before requesting use of any new information processing facilities.
- Legal/Disciplinary action shall be taken against any NSU found misusing any of the information processing facilities.

e. Management of Removable Media

Movement of media containing information will be supported by suitable authorization process.

- Movement of media will be initiated by filling up an authorization form (Gate Pass).
- In case the confidential information needs to be printed on a common printer, then a responsible person will supervise while the information is getting printed and ensure that no printouts are left on the printer.
- While transporting information media to other NSU, care will be taken to protect the media from damage, unauthorized modification. Procedure for 'Security of Media in Transit' will be followed strictly.

f. Disposal of Media

When an information media becomes unusable or not required for business, it will be disposed of securely and safely. If proper care is not taken while disposing the media, critical business information can be disclosed and misused. Procedures for disposal of media will be followed to reduce the risk of corresponding security breach.

g. **Removable Storage Devices -** USB enabled devices, such as memory sticks, external hard drives, network attached storage devices are strictly prohibited. Though there may be circumstances that require storing of sensitive and confidential information onto these utilities, it must be approved in writing, and such data is never to reside on these devices for long-term storage measures.

h. **Unknown Devices -** The phrase "unknown devices" is given to such items as kiosks, hourly computing stations for rent, friends and family members computers, or any other types of device for which [NSU] has little to no knowledge regarding its safety and security. These devices are never to be used for storing, processing or transmitting sensitive and confidential information due to the lack of knowledge of their respective encryption practices, which many times are none at all.

i. Software Licensing and Usage

It's also important to understand the company's general policy on software usage, which includes numerous responsibilities that all NSUs need to be aware of. Software is used by all of us, each and every day, as it's vital to performing daily tasks for one's job function. With that said, please be mindful of the following issues:

- **Use only approved software.** Only software approved and purchased from the company may be installed and used on any company-wide system components. This includes your workstation and any other device provided to you from the company. Unapproved software that has not been fully vetted by authorized I.T. personnel and can often contain dangerous or malicious code that's extremely harmful to computers. Simply stated, only load and use legally approved software on computers.

- **Do not duplicate software.** The licensing rights for software are strict and extremely rigid, allowing only a predetermined number of installations for a given data set. This means you are not allowed to copy or duplicate any company approved and purchased software – no exceptions. U.S copyright laws – and other regulations throughout the world – often place strict guidelines on software usage, so please keep this in mind.

- **Use caution on your own devices.** When using your own personal workstation, laptop, or other device, please consider and be mindful of the software you install, especially when such computing systems are used for potentially accessing the corporate network. While the guidelines on software for your personal computers are less restrictive, we still ask that you use extreme caution when loading any type of application onto your devices.

- **Accept updates.** For software to function efficiently and safely, security and patch updates have to be applied on a regular basis, so make sure to accept such updates when pushed out and also take time to update any software on your personal computers that do not rely on updates pushed out by I.T. personal.

- **Downloading from the Internet.** Any software obtained from the Internet is to be considered copyright protected, which means accepting any copyright agreements, and also comprehensively scanning the software for ensuring no dangerous or malicious code exists. The Internet can be an extremely dangerous forum when it comes to software as many products seem harmless, only to contain viruses that can wreak havoc on computers. Think before you start downloading any software online.

- **Software audits.** We have the right to conduct random software compliance audits on workstations, including laptops issued to you, or your own personal laptops. The audits are for ensuring compliance with software licensing rules, while also ensuring your computers are free of any potentially dangerous applications. If you're not sure what constitutes approved software, then simply ask somebody.

- **Penalties and fines.** Did you know that we as a simple use can actually be levied fines for improper software use? Yes, it's that serious and it's why we're taking the time to discuss this important issue with you. According to the U.S. Copyright Act, illegal reproduction of software is subject to civil damages up to $150,000 (Section 504(c)(1) Title 17) per title infringed, and criminal penalties, including fines of as much as $250,000 per title infringed and imprisonment of up to ten (Section 2319 (b) (2) Title 18) years.

j. Encryption

When necessary and applicable, appropriate encryption measures are to be invoked for ensuring the confidentiality, integrity, and availability (CIA) of [NSU] system components and any sensitive data associated with them. Additionally, any passwords used for accessing and/or authentication to the specified system component are to be encrypted at all times, as passwords transmitting via clear text are vulnerable to external threats. As such, approved encryption technologies, such as Secure Sockets Layer (SSL) | Transport Layer Security (TLS), Secure Shell (SSH), and many other secure data encryption protocols are to be utilized when accessing the specified system component. Additional encryption measures for [NSU] are to also include the following best practices for all applicable devices that have the ability to store sensitive and confidential information:

- **Desktop Computers -** Any desktop computer storing sensitive and confidential information are to utilize encryption for the actual hard drives. Additionally, access rights are to be limited to authorized personnel at all times. Non - [company owned] desktops, such as those physically located at a NSU, are to never contain sensitive and confidential information under any circumstances. If such data needs to be accessed for performing remote duties, then a secure connection must be made to the [NSU] network for accessing all relevant information.

Additionally, desktop computers are to be provisioned and hardened accordingly, with anti-virus also installed.

- **Laptops, Mobile Computing Devices, Smart Devices -** Such devices are to have approved encryption installed and enabled prior to their use, which requires [NSU] authorized I.T. personnel to configure appropriate encryption programs. Specifically, full disk encryption, or other approved methods, such as file level encryption are to be used, and these devices are not to be used for long-term storage of sensitive and confidential information. The phrase "long term" is discretionary in nature, but consists of any data residing on laptops, mobile computing devices, and smart devices longer than thirty (30) calendar days. Non - [NSU owned] laptops, mobile computing devices, and smart devices, are to never contain sensitive and confidential

information under any circumstances. If such data needs to be accessed for performing remote duties, then a secure connection must be made to the [NSU] network for accessing all relevant information. Additionally, laptops, mobile computing devices, and smart devices are to be provisioned and hardened accordingly, with anti-virus also installed.

k. Back-up: **Information backup and archival**

Backup copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

- The NSU shall maintain a record of all data that needs to be backed up along with the schedule for each.
- The NSU shall ensure that backup logs are reviewed on a daily basis.
- The NSU shall ensure that all backup tapes are moved to an offsite location on a daily basis.
- The NSU in co-ordination with the Administration unit shall ensure that all backup equipment and tapes are given adequate physical protection, both onsite and off-site.
- The NSU shall test all backup media once a month to test the completeness of the backup.
- The ISO shall identify suitable encryption technologies to ensure that highly confidential data is encrypted on backup tapes.
- The NSU shall ensure that the retention period of all data being backed up is identified.

l. Information handling

Information media such as tapes, document paper containing confidential information of NSU shall be maintained in safe custody, and wherever necessary, in a fireproof room. The key to that room should be available to that NSU only not they friends, etc.

ii. Computer infection

a. Anti-Virus

- ❖ All devices will have anti-virus installed, running and updated.
- ❖ NSU will not change the anti-virus settings.
- ❖ NSUs should not disable the installed anti-virus agent or change its settings defined during installation. This includes settings for daily virus scan; and signature update schedules.
- ❖ NSUs should not disrupt the auto virus scan scheduled on their desktop. If the scan is affecting system performance, NSUs should contact system administrator for resolution.
- ❖ All external media will be used only after authorization and subjected to anti-virus scan and NSUs are advised to run anti-virus scan when any external media is used.
- ❖ NSUs will report any virus detected in the system to ICT Team or to a reporting manager within respective department
- ❖ NSU must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- ❖ NSUs should exercise caution when copying files. Only download from reputable sites, and carry out a virus check on the file.

b. Turn on your firewall. Blocking suspicious traffic is essential for laptop security, so turn on and "enable" your default personal firewall or an approved personal firewall software appliance, for which there are many available.

iii. Network security

a. Use Anti-virus. It's one of the most fundamentally important – and often not used – security software, so make sure your laptop has anti-virus running at all times, along with its scanning at regular intervals for viruses, and that the software is current.

b. Wireless configuration

- ❖ Wireless router should be tested prior to selection, test should include but not limited to below points;
- ❖ Inter compatibility with other network devices
- ❖ Should support strong encryption and authentication protocol i.e.WAP2

- Should have logging mechanism
- Wireless Access Point (AP) of NSU corporate networks must not be used; it shall be used where only required and after approval from Somme IT Manager.
- All access to wireless networks shall have strong authentication mechanisms to prevent unauthorized NSUs.
- The Service Set Identifier (SSID) of the wireless device shall be configured in such manner so it does not contain or indicate any information about the organization of NSU, its departments, or its personnel including organization name, department name, NSU name, NSU phone number, email addresses, or product identifiers.
- WEP & WAP must not be used for Wireless deployment (These are vulnerable) only WAP2 with EAP-TLS
- The NSUs shall require that parts of the network containing and supporting wireless devices directly (the wireless network) be separated from the part of the network that does not support wireless connections. The part of the network supporting wireless devices or connections shall be considered less trusted than the part of the network that does not.
- Wireless access to other NSUs shall only be provided after adequate verification and authorization.
- Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in WLAN) to fully understand the wireless network security posture.
- Default Administrator password on AP must be strictly changed.

c. Network Password Use

- NSU will not keep copy of password in any written form or electronic form. If absolutely required, passwords of critical NSU accounts shall be maintained securely.
- NSUs will change passwords whenever there is any indication of possible system or password compromise.
- NSUs will change Passwords at regular intervals 90 days or based on the number of access (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid reusing or cycling old passwords.
- NSUs will change temporary passwords at first logon

- NSUs must not include password in any automated logon process, e.g.: stored in a macro or function key
- NSUs will not share their passwords with anyone.
- NSUs will ensure that nobody is watching when the password is being entered
- The NSU before to connect to the wireless access points he/she can check if is secured with help of a security key.

d. Internet Browser

- NSUs should ensure that security is enabled on the Internet browser as per guidelines given below:
    - Configure browser not to remember web application passwords.
    - Set browser security setting to medium.
- Any bundled software that the NSU has obtained with mobile phones/ Personal Digital Assistants (PDAs) etc, should be explicitly approved by reporting head and ISO.
- Institution reserves the right to monitor and review Internet usage of NSUs to ensure compliance to this policy.

e. Internet Usage

- NSUs shall not use or access the internet for non-business purposes and restrict personal use to minimum limited to educational, knowledge and news sites. NSUs should strictly avoid visiting non-business, offensive and unethical sites which violate security policies.
- NSUs should not use Internet services to:
    - Download or distribute malicious software or tools or to deliberately transmit any virus
    - Violate any copyright or license agreement by downloading or distributing protected material
    - Upload files, software or data belonging to another user to any Internet site without authorization of the owner of the file/ software/ data

- Share any confidential or sensitive information of institution with any Internet site unless authorized by Superior / Management
- NSUs shall not post any institution proprietary information or Internet share drives/Briefcase, public forums, newsrooms or bulletin boards. This is strictly prohibited and any violation will be subject to disciplinary process that includes legal consequences.
- Post remarks that are offensive/aggressive/Insulting, obscene or not in line with institution's policy on the subject.
- Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting the organization
- In case such misuse of the Internet access is detected, Authorized personnel shall terminate the NSU Internet access and take other disciplinary action.
- NSUs should ensure that they do not access websites by clicking on links provided in emails or in other websites. When accessing a website where sensitive information is being accessed or financial transactions are done, it is advisable to access the website by typing the URL address manually rather than clicking on a link.
- NSUs shall be aware that their information systems(computer, internet, email, messenger, FAX and telephone conversations),its usage and information exchanged are not private and the company reserves the right to monitor and audit these on ongoing basis and during or after any security incident.

❖ NSUs must be aware that institution accepts no liability for their exposure to offensive material that they may access via the Internet.

f. System management of NSU

❖ The System develop shall follow a formal password management process for the allocation of passwords.

❖ The System develop shall ensure that NSUs are given temporary passwords for initial login and the same shall be communicated securely.

❖ The System develop shall ensure that all default passwords provided by the vendor shall be changed following installation of system or software.

- The NSUs shall ensure that passwords are not stored on computer systems in an unprotected form.
- The System develop shall define procedures for password resets.
- The NSUs shall follow complexity guidelines in the selection of passwords to ensure their quality.
- The System develop shall implement controls to change passwords at a frequency of 90 days.
- The System develop shall ensure that password history of previous passwords is maintained to prevent re-use.
- The System develop shall ensure that all the systems, applications will adhere to password policy.
- The System develop shall ensure that all passwords are kept confidential and not shared unless otherwise authorized by the ISO if there is a business reason.

g. Termination or change of Asset

- In case of termination, a clearly defined exit procedure will be followed and a record of the same will be maintained. This will include the return/review of all previously issued information and information processing assets.
- The access rights of all NSU to information and information processing facilities will be removed on termination of their employment / contract /agreement or modified for any change in their designation / status.
- All NSUs should return all NSU assets in their possession upon termination of their employment, contract or agreement.
- If the NSU are outgoing in their institution or organization, he /she can check if they personnel documents are removed and deleted in the organization computer.

h. Communication and operations management

The purpose is to ensure secure processing, storage and movement of NSU's information through adequate planning, operating procedures, backup, change management, media handling and

network management. All the information, its communication and processing facilities, flow of information within NSU and outside NSU will be protected by appropriate system / network planning, management and through well-established operating procedures.

- Operational procedures and responsibilities

Operating procedures for information systems will be repressed and authorized by the NSU and will be made available to all NSUs who need them. These procedures include:

- Networking equipment start up and close down
- Backup
- Equipment maintenance
- Media handling, computer room and mail handling management, and safety.

Operating procedures require specifying the instructions for the detailed execution of each job including the interdependencies, if any, and instructions for dealing with exceptions or errors that may arise during job execution.

i. Equipment identification in networks of NSU

- The Network configure shall ensure that connection to network devices for administrative purposes is identified through an IP Address or MAC Address.
- The Network configure shall ensure that all network devices are configured to control access to and from the network using identifiers such as IP Addresses or MAC Addresses
- Network Access Control (NAC) may be considered for auto identification of devices on the network.
- Any new devices connected to the NSU networks shall be identified and monitored

j. Remote diagnostic and configuration port protection

- The NSU shall ensure that all servers (if he/she has localhost) and network equipment are placed in locked cabinets/rooms to prevent the direct access to remote diagnostic ports.
- The NSU shall ensure that all default enabled ports and services that are not required for business purposes are disabled.

k. Network Connection Control

- The Network admin shall ensure that access control rules are implemented on the network devices to ensure that NSUs access to information services such as email, file transfer, etc. are controlled.
- Where possible the Network admin shall ensure that Internet services are restricted and available during the NSU hours work only.

l. Network Routing Control

- The Network admin shall ensure that controls are applied on Internet firewalls to hide the IP address schema used by NSU.
- The Network admin shall ensure that filters are applied on the Internet router or Internet firewalls to ensure any "internally" reserved IP address does not appear as the source at the externally facing interface.

m. Secure log-on procedures

- All NSUs, applications and Network Devices must be secure and traffic encrypted using technologies such as SSH, SSL, Tokens, etc...
- The use of weak log-on procedures(e.g.: telnet) is prohibited while accessing NSU Systems, Applications and Networks Devices
- The NSU shall ensure that access to information services is controlled by secure log-on process.
- The log-on procedure should disclose minimum of information about the system, in order to avoid providing an unauthorized NSU with unnecessary assistance.

n. NSU identification and authentication

- The ICT team shall ensure that all the NSUs have a unique NSU ID.
- The ICT Team shall ensure that prior management approval is taken for creating shared NSU ID and generic ID.
- The NSUs shall ensure that a strong password is used for authentication.
- By default any new NSUs shall have minimum level of privileges, higher privileges required for job shall be expectedly approved by reporting manager.

- Use of system utilities:The ICT team shall restrict and control the use of utility programs that might be capable of overriding system and **application controls.**

o. Session time-out

- The NSU shall ensure that all computing equipment's are configured to lock after 5 minutes of inactivity.
- The NSU shall ensure that wherever feasible, all inactive sessions are configured to shut down after a period of 10 minutes.

p. Limitation of connection time

- The NSU shall enforce restrictions on connection time for sensitive applications to normal office hours if there is no requirement for over-time or extended-hours of operation.
- The NSU shall enforce re-authentication at timed intervals.

q. Information Access Restriction

- The Application Owner shall ensure that the access to information through the applications is controlled by the use of menus. The menus shall be designed such that access to sensitive information is controlled through the use of a password.
- The Application Owner shall ensure that NSUs are given varied access rights e.g. read, write, execute depending on his/her business requirement.

X. Sensitive System Isolation

- The NSU shall define and document the sensitivity of the application in terms of Confidentiality, Integrity and Availability.
- The ISO shall conduct a risk assessment on an annual basis of all those applications that are critical to the business and that run on shared environments.
- Application Owners shall require to formally approve the sharing of environments for critical business applications.
- Critical information systems shall be strongly secure and isolated to the rest of other systems

y. Mobile Computing and Communications

- All NSUs using mobile computing devices such as laptop, smart phones, Ipad and similar hand held devices for business purposes or store data shall be trained on the security best practices towards these devices.
- A risk assessment shall be performed on the potential threats associated with the various forms of mobile computing for new devices that become available.
- NSUs of mobile computing devices (i.e. laptop, smart phones, Ipad and similar hand held devices) shall be required to sign a statement of their understanding and compliance to the mobile computing policy.
- NSUs shall reasonably ensure mobile devices are physically secure at all times if they contain their sensitive data.

Examples of physically securing devices include: mobile devices should never be left visible in a car, and should never be left in the trunk or other storage location overnight. Mobile devices should always be carried on-board aircraft and not put in checked luggage if a mobile device contains other than NSU data, it shall have some form of access control (e.g. NSUname and password) to access this information. If access to the device is not controllable, access to the data must be controlled.

- If a mobile device contains sensitive NSU, it shall be encrypted on the storage drive. Encryption may be on a file-by-file basis, or on a volume-by-volume basis.
- NSUs are strongly encouraged to back up their data stored on mobile devices. Backup may be done when connected to their network (file shares and other backup facilities), or may be backed up to removable media. If backed up to removable media, this media must be physically protected or the data must be encrypted.
- Remote connections to the institution network shall be made from mobile devices at public places only after obtaining prior approval from the respective division / unit manager, infrastructure owner.
- Before connecting to the NSU network from the public network, the following points shall be considered:
    - NSUs must use an approved personal firewall, and have it running and actively filtering traffic, when connecting to networks from public places.
    - NSUs must also have current and active anti-virus software running before connecting.
    - Remote connections will be made through VPN tunnels to safeguard the connection traffic.

iv. Transmission of data

The procedures, and controls of transmission of data shall be in place to protect the exchange of information through the use of all types of communication facilities”

- Appropriate controls will be implemented for protection against malicious code, while transmitting information electronically.
- Sensitive information will be protected using encryption, password or any other suitable method especially when being sent as an attachment in an email.
- Disposal procedures will be followed to destroy sensitive information.

a. The end NSUs

- Not leave sensitive information unattended at fax machines, printers etc.
- Not auto-forward mails to external mail ids.
- Not reveal sensitive information in public
- Not leave sensitive messages on answering machines
- Check the recipients email id/fax number before sending an email or a fax respectively.

- **Information exchange**

In case of an exchange of information between NSUs, appropriate agreement will be established addressing the following points:

- Traceability and non-repudiation
- Courier identification standards
- Responsibilities and liabilities in the event of an incident
- Labelling system as per the sensitivity of the information
- Cryptography
- Appropriate controls will be implemented for protection against malicious code, while transmitting information electronically.
- Sensitive information will be protected using encryption, password or any other suitable method especially when being sent as an attachment in an email.
- Disposal procedures will be followed to destroy sensitive information.

- The NSUs will,
    - Not leave sensitive information unattended at fax machines, printers etc.
    - Not auto-forward mails to external mail ids.
    - Not reveal sensitive information in public.
    - Not leave sensitive messages on answering machines.
    - Check the recipients email id/fax number before sending an email or a fax respectively.

b. Electronic messaging

- Information present in electronic messages will be appropriately protected according to its criticality.
- Confidential Emails will be encrypted and attachments will be password protected for information passing over the publicly accessible networks.

c. Business Information Systems

Interconnection of Business information / communication systems including phone calls, conference calls, facsimiles, Emails etc. shall be adequately protected.

d. Electronic commerce services: Publicly available information

The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

- Unauthorized modifications to electronically published information on NSU's website may harm its reputation. System Administration Team or website design will implement appropriate controls to protect this information from unauthorized access. NSU would be the internal authority for the content proposed to be published - on website.

- It will be ensured that the information to be published is in compliance with applicable legislation and contractual obligations. The data collection over web will also comply with the applicable legislation.

e. Secure Log-on Procedures

- ICT Team shall develop guidelines for secure exchange of information.
- The Information Security Team shall communicate these guidelines to all the NSUs of Institution's information systems on an annual basis via the information security awareness sessions.

f. Reporting Information Security Incident and Weaknesses

- All users of institution should be aware or made aware of their responsibility to report any information security incidents and / or weaknesses in systems or services.
- All users shall report Information security related events and weaknesses through the quickest mode to the ICT department.

g. Prevention of misuse of information processing facilities

- All users of institution should use the information processing facilities for business purposes only.
- Any use of these facilities for non-business purposes without management approval or for any unauthorized purposes, should be regarded as improper use of facilities or breach of confidentiality. The unauthorized activity may be identified by monitoring or other means.
- Intrusion detection, intrusion prevention, content inspection, and other monitoring tools shall be used to detect and prevent misuse of information processing facilities.

i. NSU Privacy

NSUs should have no expectation of privacy while using company-owned or company leased equipment. Information passing through or stored on company equipment can and will be monitored as and when required for security and compliance reasons.

m. Email Usage

1 Email is a business communication tool and NSUs must use this tool in a responsible, effective and lawful manner.
2 NSUs shall comply with institution's E-mail policy on proper and effective use of E-mail.
3 NSUs shall archive his/her emails on regular intervals. NSUs should protect their email account on the server through strong password and should not share their password or account with anyone else. All such locally stored emails on critical laptops/ desktops shall be protected by a password.
4 NSU shall conduct the necessary housekeeping of his/her email at regular interval.
5 NSUs should promptly report all suspected security vulnerabilities or problems that they notice with the email system to the designated ICT Team and or ISO.
6 Institution has the authority to intercept or disclose or assist in intercepting or disclosing E-mail communications.
7 NSUs will not use any email account other than the one provided by institution for transacting official information.
8 Confidential information will be secured before sending through e-mail by way of compression, password protection or other advanced cryptographic means.
9 Language used should be consistent with other forms of business communications
10 NSUs should treat electronic-mail messages with sensitive or confidential information as 'Confidential' and take due care as per the' information handling guidelines'.
11 NSUs shall avoid opening mail from unknown NSUs/sources and also avoid opening suspicious attachments or clicking on suspicious links.
12 Shall restrict attachments size on the company mail system. Outgoing mail sizes are restricted to less than **5 MB.**

13 NSUs shall avoid sending or forwarding unsolicited email messages; “chain letters”, “Jocks”, “junk mail”, etc…. from other internal NSUs and external networks or other advertising material to individuals who did not specifically request such material (email spam).

14 NSUs shall avoid any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

15 NSUs shall avoid unauthorized use, or forging, of email header information.

n. Change Management

- Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all changes to equipment, applications and procedures are required to be followed.
- Change management form needs to be completed for each scheduled, unscheduled or emergency change following the steps contained in the Change Management Procedures.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log will be maintained for all changes. The log must contain, but is not limited to:
    - Date of submission and date of change
    - Owner and custodian contact information
    - Nature of the change
    - Indication of success or failure