Information Technology Policy of NTA, 2080 (2023)

Whereas, it is expedient to outline the guidelines, rules, and responsibilities for the use of technology resources and information systems within the organization, Nepal Telecommunications Authority (hereinafter referred to as “NTA”) has formulated and issued this Information Technology Policy. The policy aims to ensure the data and information assets' confidentiality, integrity, and availability while promoting responsible and ethical use of technology resources. All NTA members, employees, contractors, vendors, consultants and authorized users shall adhere to this policy.

Chapter – 1
Preliminary

1. **Title**: (1) This policy may be called “IT Policy of NTA, 2080 (2023)”.
   (2) This policy shall come into force immediately.
2. **Definition**: Unless the subject and context otherwise require, in this policy:
   (i) “Act” means the Telecommunication Act, 2053 (1997).
   (ii) “Authority” or “NTA” means Nepal Telecommunications Authority established pursuant to the Act.
   (iii) “Chairman” means the chairman of the Authority.
   (iv) “Contractor” means a person or firm that undertakes a contract to provide goods or services to NTA.
   (v) “Coordinator” means the coordinator of IT Coordination Committee.
   (vi) “Employee” means employee working on a permanent post of NTA.
   (vii) “Information System Owner” means the Head of Division/Section that is operating the Information System.
   (viii) “IS” means Information System that are owned by NTA.
   (ix) “IT” means Information Technology.
   (x) “Non-Disclosure Agreement” or “NDA” means a legally binding confidentiality agreement between NTA and contractor/vendor in which one party gives a second party confidential information about the business and the second party agrees not to share the information with anyone else.
   (xi) “NTA Member” means the member of the Authority and the term also includes the Chairman.
   (xii) “Remote Access” means the access of a computer or network from a geographical distance through internet connection.
   (xiii) “SSL” means Secure Sockets Layer encryption.
   (xiv) “User” means all NTA members, employees, contractors, vendors, consultants, and authorized person who uses the IT resources of NTA.
   (xv) “Vendor” means a person or company that sells a good or software product to NTA.

Chapter - 2
Acceptable Use Policy

3. **General Usage**: (1) NTA proprietary information stored on electronic and computing devices whether owned or leased by NTA, the employee, or a third party, remains the sole property of NTA. Users must ensure through legal or technical means that proprietary information is protected in accordance with the statutory Data Protection Standard of Nepal.

   (2) Users have a responsibility to report the theft, loss, or unauthorized disclosure of NTA's proprietary information immediately to the head of the Coordination Committee as specified in **Annex – 1**.

   (3) Users may access, use or share NTA proprietary information only to the extent as authorized and necessary to fulfill the assigned job duties.

   (4) For security and network maintenance purposes, NTA authorized personnel may monitor equipment, systems, and network traffic of NTA at any time as during NTA's Information Security Audit.

4. **Prohibited Activities**: The following activities are strictly prohibited and may result in a disciplinary action:
   (a) Unauthorized access, use, or disclosure of NTA's confidential information/ data.
   (b) Installation of viruses, or other malicious software and injection of malwares.
   (c) Hacking, cracking, or any attempt to compromise system security.
   (d) Unauthorized sharing or distribution of confidential or proprietary information.
   (e) Violation of intellectual property rights, including software piracy.
   (f) Inappropriate or offensive use of technology resources, including harassment or discrimination.
   (g) Unauthorized modification or deletion of NTA's data or systems.
   (h) Use of technology resources for illegal activities.

Chapter - 3
Domain

5. **Primary Domain**: (1) The primary domain of NTA is nta.gov.np. The domain shall be used on the official website and email of NTA.

6. **Subdomain**: (1) For various web-application of NTA and its corresponding email service, the NTA shall use the appropriate sub-domain under the primary domain.

   (2) The sub-domain name shall be approved by the Chairman.

   (3) The sub-domain in use prior to this policy shall be assumed to have been approved as per this policy.

   (4) The IT Division shall main the record of the sub-domain as per Annex-2 mentioning handover details.

   (5) NTA shall manage a single wildcard SSL Certificate from a trusted Authority that will be valid for the primary domain and all its sub-domains.

   (6) IT Division shall provide the SSL Certificate to all concerned divisions/sections.

Chapter – 4
Email Accounts Policy

7. **Email Account**: (1) NTA shall use the primary domain (*@nta.gov.np*) for its email.

(2) NTA might use the email service under a sub-domain for a specific purpose.

(3) An NTA email under the primary domain will be of three types: (a) Functional Email (b) Personal Email (c) Group Email.

(4) IT Division is responsible for creating, modifying, deactivating and deleting an email account.

(5) NTA shall have following three categories of email accounts:

(a) Functional Email:

- The functional email shall be used for specific purposes.
- Creation of a functional email requires approval from the Chairman.
- The IT Division shall handover a functional email to the respective division/ section after keeping the record as per Annex-3.

(b) Personal Email:

- NTA shall provide personal email to the chairman, members, and employees.
- The personal email will be of the form:
  Initial of First Name + Initial of Middle Name (if any) + Last Name + @nta.gov.np
  If the email id is already in use, IT Division will create an appropriate email id in consultation with the concerned person.
- The IT Division shall handover a personal email to the respective person after keeping the record as per Annex-4. The creation of a personal email does not require approval from the chairman.

(c) Group Email:

- The group email shall be used to forward email to all users belonging in a group.
- The email shall be based on the designation and service group only.

Chapter – 5
Email Usage Policy

8. **Acceptable use of Email**: Employees shall use NTA's email accounts primarily for official business purposes and professional communication related to their job responsibilities. Personal or non-work-related emails shall be kept to a minimum.

9. **Appropriate Content**: (1) Employees must use good judgment and ensure that all email communications are professional, respectful, and in compliance with policies of NTA.

(2) Offensive, discriminatory, or harassing content is strictly prohibited.

10. **Confidentiality and Data Protection: (1) Employees must exercise caution when** sending emails containing confidential or sensitive information by adding "**for confidential (internal or as per sensitivity) use only**".

(2) Confidential information shall be appropriately encrypted or password-protected before transmission, and access to such emails shall be limited to authorized recipients.

11. **Proper Identification**: (1) Employees shall clearly identify themselves in all email communications, including their full name, job title, and official contact information. Impersonating others or using false identities is strictly prohibited.

    (2) Employees might use their digital signature in the email communication as per need.

12. **Email Security**: (1) Users must ensure the security of their email accounts by using strong, unique passwords.

    (2) Users shall refrain from sharing their login credentials with others.

    (3) Password shall be changed periodically.

    (4) Users shall not use their official email for registration or Log-in process in websites which are not related with NTA's policies.

13. **Email Retention and Deletion**: (1) Users shall adhere to an email retention policy, which outlines the duration for which emails shall be retained.

    (2) Emails that are no longer required for business or legal purposes shall be promptly deactivated to reduce storage and security risks.

Chapter – 6
User Management and Access Control Policy

14. **User Account Creation**: (1) User accounts shall be created for authorized individuals based on their job responsibilities and the principle of least privilege.

    (2) User account creation shall follow a formal process that includes verification of identity and approval from appropriate managers or system administrators.

15. **Account Provisioning:** (1) User accounts shall be provisioned promptly upon joining the authority.

    (2) Provisioning includes granting appropriate access rights and permissions based on job roles and responsibilities.

16. **Account Termination:** (1) User accounts must be deactivated or removed promptly when an employee/vendors/consultants/ contractor leaves the Authority or when access is no longer required.

    (2) Account termination shall be part of the employee off-boarding process and follow a formal procedure to ensure the removal of access rights.

17. **Role-Based Access Control (RBAC):** (1) Access privileges shall be assigned based on job roles and responsibilities.

    (2) RBAC shall be implemented to ensure that users have the necessary access required to perform their duties and nothing beyond that.

18. **Principle of Least Privileges:** (1) This policy aims to minimize the risk of unauthorized access, data breaches, and misuse of resources by granting users only the privileges necessary to perform their job responsibilities.

    (2) It shall be ensured that the information system prevents the non-privileged users from executing privileged functions including disabling, circumventing, or altering implemented security safeguards/countermeasures.

19. **Separation of Duties:** (1) Critical business processes shall be divided among multiple individuals to prevent any single person from having excessive control or access.

(2) Sensitive functions, such as financial transactions or data manipulation, shall require multiple approvals or involvement from different individuals.

(3) The duties of individuals shall be separated as necessary to prevent malevolent activity without collusion.

(4) The separation of duties of individuals shall be documented by IT Division.

20. **Access Monitoring and Logging:** (1) Access to systems, applications, and sensitive data shall be logged and monitored by IT Division/Section for security and compliance purposes.

(2) Security logs shall be reviewed regularly to identify any unauthorized access attempts or suspicious activities.

21. **Control of Unsuccessful Login Attempts:** (1) The number of consecutive invalid login attempts shall be limited to a defined number.

(2) The user account that exceeds the limit of consecutive invalid login attempts will be suspended for a certain interval of time or until released by an administrator.

(3) Only the administrator shall have permission and privilege to unlock such a suspended account.

22. **System Use Notification:** The information system shall display to users an approved system uses notification message or banner before access to the system that provides privacy and security notices, stating**:**

(a) Users are accessing an NTA's information system.

(b) Information system usage may be monitored, recorded, and subject to audit.

(c) Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

(d) Use of the information system indicates consent to monitoring and recording.

(e) There are no rights to privacy while accessing the information system.

23. **Remote Access**: (1) IT Division shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

(2) Any remote access to the information system by a third party shall be authorized by IT Division prior to allowing such connections and Log-in details shall be recorded by IT Division.

(3) IT Division shall ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

(4) IT Division shall document the rationale for such access in the security plan for the information system.

24. **Publicly Accessible Content:** (1) NTA shall designate officers authorized to post information onto a publicly accessible information system.

(2) The authorized officers shall be trained to ensure that publicly accessible information does not contain nonpublic information.

(3) The authorized officers shall review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

(4) The authorized officers shall remove any non-public information from the publicly accessible information system as soon as it is discovered.

Chapter – 7
Identification and Authentication Policy

25. Identification and Authentication Mechanism: (1) Information system shall have a mechanism to uniquely identify and authenticate users or processes acting on behalf of the authenticated users.

(2) IT Division shall ensure that information systems implement multifactor authentication for network access to privileged accounts.

(3) There shall be a mechanism to enhance the security of systems and protect sensitive information from unauthorized access or breaches.

26. Requirement for Strong Password: (1) Users must create passwords that are strong and difficult to guess.

(2) Passwords must contain characters from three of the following categories:

(a) Uppercase character (A through Z)
(b) Lowercase character (a through z)
(c) Base 10 digits (0 through 9)
(d) Non-alphanumeric characters such as !, @, #, $, %, & etc.
(e) Any Unicode character that is characterized as an alphanumeric character

(3) Passwords shall be at least 8 characters long to provide a sufficient level of complexity and security.

(4) At least one character must be changed when a new password is created.

27. Unique Passwords: (1) Users shall not reuse passwords across multiple systems or accounts.

(2) Reuse of personal passwords in NTA IS and NTA IS passwords in personal accounts is prohibited.

(3) Each account or system shall have a unique password to prevent unauthorized access in case of a password compromise.

28. Password Protection and Storage: (1) Users must keep their passwords confidential and not share them with others, including colleagues or family members. Passwords shall not be written down or stored in easily accessible locations, such as on sticky notes, notebooks or in unsecured digital files (e.g. Plain text file).

(2) All passwords must be cryptographically protected while stored and transmitted.

(3) Two-Factor Authentication: Where available, two-factor authentication (2FA) shall be enabled for accounts to provide an additional layer of security.

(4) Password Managers: Employees are encouraged to use trusted password manager applications or built-in browser password managers to securely store and manage their passwords.

Chapter – 8
Hardware and Physical Device Policy

29. Hardware Policy: (1) All the devices used within the authority must be ensured to be trusted and shall meet the standard requirement of the authority.

(2) NTA strictly prohibits the use of faulty hardware which may posses' risk of power outage, power failures and so on. If employee is found intentionally causing any type of risk to the authority assets, he/she is liable to legal action.

(3) All the employees are instructed to use the hardware of the organization as far as possible.

(4) If the employee choses to bring their own devices, then it must be verified by the organization as safe to use within organization premises.

But this provision is not applicable for the personal mobile devices.

(5) The Authority requires the devices used by the employees to be registered in NTA' records.

(6) The employees responsible for maintaining the hardware day to day activities must check the condition of the hardware and ensure it is working properly. They are instructed to report even the slightest abnormality found in hardware condition or operation to the respective authority.

(7) Employees are strictly forbidden to grant access to hardware device to a third party without the permission of the Chairman.

30. Physical Device Policy: (1) All the device belonging to NTA are to be kept securely by the employees in cases of intentional physical damage, loss or theft of devices the employee themselves will be held responsible.

(2) In case of hardware replacement, proper information must be passed to NTA and the damaged or replaced hardware must be presented to the NTA.

(3) Proper security mechanism such as cameras, biometric locks or some similar features decided by the organization must be implemented in the room responsible for hardware storage. The person in-charge and access to this room is responsible for keeping all these devices safe and ready for questioning anytime in case of any uncertainty.

(4) Proper care must be taken while disposing the damaged hardware. A proper record of the problem due to which hardware was disposed and method used for disposal must be mentioned while disposing the hardware.

Chapter – 9
Software Installation and Usage Policy

31. Software Installation: (1) Software must be selected from an approved software list, maintained by the IT Division unless no selection on the list meets the requester's need.

(2) Software requests must first be approved by the requester's manager and then be made to the IT Division in writing or via email.

(3) IT Division will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

32. Software Usage: (1) The use of pirated software/applications is prohibited.

(2) Sharing of a software or its license is not allowed unless approved.

(3) User shall transfer a software and/or software license only during job rotation or job termination.

33. **Prohibition on Software Usage**: NTA might block the use of certain software as and when deemed necessary.

Chapter – 10
Website and Web Application Policy

34. **Policy for Website/App Developers and Management**: (1) Only those employees who have clearance to access the website's back or front end are eligible to access the website.

(2) Developers must ensure that access to the website is not provided to anyone else other than themselves without authorization of the authority.

(3) While using any content management software, it must be ensured that it is up to date and does not possess any risk to the authority.

(4) Developers must ensure that while updating any content of the website prior authorization of the authority is given.

(5) If a third party is involved in using the website, then a report regarding all the people who have access to the website must be maintained by IT Division and given to the authority.

(6) Third parties must also maintain a report regarding all the activities that were done while using the website.

(7) Until and unless instructed by NTA to do so, no users are allowed to access the backend of the website from any other place other than NTA's office premises.

(8) NTA has the right to monitor any device by which the website was edited or updated and if instructed by the organization employees must provide his/her device to the authority for inspection

(9) It must also be ensured that the device which accesses the website must be free from viruses, malware, spyware, or any similar kind of software.

(10) While accessing website if activities other than the ordinary are observed like site being slow, information being not updated, unwanted content occurring and so on, such incidents shall be immediately reported by the employees/developers to their superior/IT division.

Chapter – 11
Information System and Services Development and Acquisition Policy

35. **Allocation of Resources**: IT Division, in coordination with the information system owner, shall:

(a) Determine information security requirements for the information system or information system service during planning phase.

(b) Determine, document, and allocate the resources required to protect the information system or information system service.

(c) Create a separate line item for information security in organizational planning and budgeting documentation.

36. **System Development Life Cycle**: IT Division, in coordination with the information system owner, shall develop a contingency plan for the information system that:

(a) Manages the information system using the system development life cycle to ensure information security considerations are taken into account.

(b) Defines and documents information security roles and responsibilities throughout the system development life cycle.

(c) Identifies individuals having information security roles and responsibilities.

(d) Integrates the information security risk management process into system development life cycle activities.

37. **Acquisition Process**: IT Division shall ensure the acquisition process includes the following requirements, descriptions, and criteria in the acquisition contract for the information system, system component, or information system service in accordance with applicable laws, policies, regulations, standards, guidelines, and business needs:

(a) Security-related functional, strength, and assurance requirements.

(b) Security-related documentation requirements.

(c) Description of the information system development environment and environment in which the system is intended to operate.

(d) Acceptance criteria.

38. **Information System Documentation**: (1) Information System Owner shall obtain administrator documentation for the information system, system component, or information system service that describes:

(a) Secure configuration, installation, and operation of the system, component, or service.

(b) Effective use and maintenance of security functions/mechanisms.

(c) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

(2) Information System Owner shall obtain user documentation for the information system, system component, or information system service that describes:

(a) User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.

(b) Methods for user interaction that allow people to use the system, component, or service in a more secure manner.

(c) User responsibilities in maintaining the security of the system, component, or service.

(3) Information System Owner shall document any attempts made to obtain documentation for information system, system component, or information system service when such documentation is either unavailable or nonexistent.

(4) Information System Owner shall protect documentation as required, in accordance with the risk management strategy.

(5) Information System Owner shall distribute documentation to only authorized persons or entities.

39. **Developer Configuration Management**: (1) IT Division, in coordination with the Information System Owner, shall ensure developers of the information system, system component, or information system service to:

(a) Perform configuration management during system, component, or service design; development, implementation, and/or operation.

(b) Document, manage, and control the integrity of changes to configuration items under configuration management.

(c) Implement only organization-approved changes to the system, component, or service.

(d) Document approved changes to the system, component, or service and the potential security impacts of such changes.

(e) Track security flaws and flaw resolution within the system, component, or service and report findings to authorized personnel and/or business units.

(2) IT Division and Information System Owner shall require the developer of the information system, system component, or information system service to enable verification of integrity of software, firmware and hardware components.

40. **Developer Security Testing and Evaluation**: IT Division, in coordination with the Information System Owner, shall require the developer of the information system, system component, or information system service to:

(a) Create and implement a security assessment plan.

(b) Perform unit, integration, system, regression testing/evaluation.

(c) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.

(d) Correct flaws identified during security testing/evaluation.

(e) Identify common vulnerabilities/flaws and document the results of the analysis using static code analysis tools.

(f) Perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

Chapter – 12
Vendor Management Policy

41. **Responsibility of NTA in Vendor Management**: (1) All the Vendors who are granted access to NTA's Information Resources must sign the Non-Disclosure Agreement (NDA). A reference NDA is attached in Annex – 5.

(2) All the Vendors must be evaluated prior to the start of any service and thereafter on an annual basis.

(3) A thorough vendor risk assessment must be performed on vendors with physical or logical access to confidential information of NTA.

(4) Vendors with compliance requirements must have their status reviewed on an annual basis.

42. **Responsibility of Vendor**: (1) If a vendor subcontracts part of the information and communication technology service provided to NTA, the vendor is required to ensure appropriate information security practices throughout the supply chain and to notify NTA.

(2) All the Work outside of defined parameters in the contract must be approved in writing by NTA.

(3) All Vendor performance must be reviewed annually to measure compliance to implemented contracts or SLAs. In the event of non-compliance with contracts or SLAs regular meetings will be conducted until performance requirements are met. If the chairman deems the services unfit NTA has full right to terminate the contract.

(4) All vendors are to strictly follow the instruction mentioned in Non-disclosure agreement. In the event of non-compliance with NDA, meeting will be conducted to make sure all compliance is met and, in such event, NTA has full rights to terminate the contract.
(5) Vendor's major IT work activities must be entered or captured in a log and made available to NTA management upon request. Logs must include, but are not limited to, events such as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
(6) Any other NTA information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.
(7) Vendor personnel must report all security incidents directly to NTA within the time frame defined in the contract.
(8) Vendor must provide NTA a list of key personnel working on the contract.
(9) Vendors who have logical access to information resources must provide non-repudiation authentication mechanisms.
(10) Vendors must notify NTA of key staff changes within 24 hours of change.
(11) Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to NTA or destroyed within 24 hours.
(12) Upon termination of contract, vendors must be reminded of confidentiality and non-disclosure requirement
(13) Upon termination of contract or at the request of NTA, the vendor must surrender all NTA badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized NTA management.

Chapter – 13
Physical and Environment Protection Policy

43. Physical Access authorizations: IT Division shall:

(a) Develop, approve, and maintain a list of individuals with authorized access to the facilities where the information systems reside.
(b) Issue authorization credentials for facility access.
(c) Review the access list detailing authorized facility access by individuals and remove individuals from the facility access list when access is no longer required.

44. Physical Access Control: The Administration Division shall

(a) Enforce physical access authorizations by verifying individual access authorizations before granting access to the facility.
(b) Control ingress/egress to the facility using secure physical access control systems/devices and/or guards.
(c) Maintain physical access audit logs for all entry/exit points.
(d) Provide secure safeguards to control access to areas within the facility officially designated as publicly accessible.
(e) Escort visitors and monitor visitors' activity within the NTA office premise and sites where NTA IT Systems resides.

(f) Secure keys, combinations, and other physical access devices.

45. **Visitor Access Records**: The IT Division shall maintain visitor access records to the facility where the information system resides for a whole year; and reviews visitor access records once a month. The visitor access record must contains the name, organization, designation, email, contact number, government id of the visitor along with the entry and exit time followed by the signature of the visitor.

46. **Power Equipment and Cabling**: The IT Division, in collaboration with Administrative Division, shall:

(a) Protect power equipment and power cabling for the information system from damage and destruction.

(b) Determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources.

47. **Emergency Power**: The IT Division shall:

(a) Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system; the transition of the information system to long-term alternate power in the event of a primary power source loss.

(b) Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

48. **Fire Protection**: The Administration Division shall employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source. This applies primarily to facilities containing concentrations of information system resources including, for example, data centers and Server/Computer rooms.

49. **Water Damage Protection**: The Administration Division shall protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Chapter – 14
Coordination Committee

50. **Formation of Coordination Committee**: (1) To ensure the implementation of the policy and to coordinate between the IT Division and various divisions/sections of NTA, a coordination committee comprising the following members shall be formed:

a.	Director, IT Division	- Coordinator
b.	Deputy Director, IT Division	- Member
c.	Deputy Director, HRD and IA Section	- Member
d.	Assistant Director, IT Division	- Secretary

(2) The meeting of the committee shall be held at such place, date, and time as specified by the coordinator.

(3) The committee can invite NTA staff and experts in the meeting.

(4) The members of the committee and invitees shall be provided meeting allowances as per the NTA's rule.

Chapter – 15
Miscellaneous

51. Training and Awareness: (1) IT Division, in coordination with the Human Resources Development and Internal Administration Section, shall regularly organize training and awareness programs related to IT to the employees of the Authority.

(2) IT Division, in coordination with the Human Resources Development and Internal Administration Section, shall schedule IT related awareness and training as a part of initial training for new employees.

(3) IT Division shall determine the appropriate content of the training and awareness programs.

52. IT related Procedures: NTA may formulate IT related procedures to implement this policy.

53. Power to remove difficulties: If any difficulties arises in the implementation of this policy, NTA may issue necessary order to remove such difficulties without any inconsistency with the provisions of this policy.

Annex – 1

Incident Report Form

To,
The Chairman,
Nepal Telecommunications Authority.

Subject: Reporting of Incidence

Dear sir/madam,
I would like to report you an incident as mentioned below:

Incident Details: ____

____

____

Incident Site (System/Device): ___________________________________

Incident Time (Approximately): __________________________________

Log, Screenshot etc.: ____

Name of Reporting Employee: ___________________________________

Signature of Reporting Employee: ________________________________

I seek your support for the rectification of the same.

Thank you.

Yours Sincerely,
…………………

Enclosures:

(a) Log files
(b) Screenshots

Annex – 2

Record of Sub-domain of NTA

SN	Sub-Domain Name	Purpose	Responsible Department or Section	Effective Date of Implementation	Handover Details	Remarks

Annex – 3

Record of the Functional Email of NTA (including Handovers)

Email Address of Functional Email: ____
Purpose of the Email: ____
Responsible Department or Section: ____
Date of Creation or Handover: ____
Handover Details: ____
Name of Employee (who created email account): _____________________________________
Signature of Employee (who created email account): __________________________________

I certify that I have received the login credentials of the email account assigned to me. I shall use this email account for the official use only, as per the IT policy of NTA.

(Receiver Employee)
Name: ____
Designation: ____
Current Section/Department: ___________________________

Annex – 4

Record of the Personal Email of NTA

Personal Email Address: ____
Name of the Employee: ____
Date of Creation: ____
Handover Details: ____
Name of Employee (who created email account): _________________________________
Signature of Employee (who created email account): ______________________________

I certify that I have received the login credentials of the email account assigned to me. I shall use this email account for the official use only, as per the IT policy of NTA.

____

(Receiver Employee)

Name: ____
Designation: ____
Current Section/Department: ___________________________

Annex – 5

NEPAL TELECOMMUNICATION AUTHORITY

NON-DISCLOSURE AGREEMENT

THIS AGREEMENT (the "**Agreement**") is entered into on this ____day of ___________ by and between ________________, located at ___________________ (the" **Disclosing Party"**), and ____________________________ with an address at ______________________ (the "**Receiving Party"**).

The Receiving Party hereto desires to participate in discussions regarding ________________________ (the "**Transaction**"). During these discussions, Disclosing Party may share certain proprietary information with the Receiving Party based on the company's policies. Therefore, in consideration of the mutual promises and covenants contained in this Agreement, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties here to agree as follows:

1. **Definition of Confidential Information**.

(a) For purposes of this Agreement, "**Confidential Information**" means any data or information that is proprietary to the Disclosing Party and not generally known to the public, whether in tangible or intangible form, **in whatever medium provided, whether unmodified or modified by Receiving Party or its Representatives (as defined herein),** whenever and however disclosed, including, but not limited to: (I) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated companies; (ii) plans for products or services, and customer or supplier lists; (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, information and trade secrets; (v) any other information that shall reasonably be recognized as confidential information of the Disclosing Party**; and (vi) any information generated by the Receiving Party or by its Representatives that contains, reflects, or is derived from any of the foregoing.** Confidential Information need not be novel, unique, patentable, copyrightable or constitute a trade secret in order to be designated Confidential Information. The Receiving Party acknowledges that the Confidential Information is proprietary to the Disclosing Party, has been developed and obtained through great efforts by the Disclosing Party and that Disclosing Party regards all of its Confidential Information as trade secrets.

(b) Notwithstanding anything in the foregoing to the contrary, Confidential Information shall not include information which: a) was lawfully possessed, as evidenced by the Receiving Party's records, by the Receiving Party prior to receiving the Confidential Information from the Disclosing Party; (b) becomes rightfully known by the Receiving Party from a third-party source not under an obligation to Disclosing Party to maintain confidentiality; (c) is generally known by the public through no fault of or failure to act by the Receiving Party inconsistent with its obligations under this Agreement; (d) is required to be disclosed in a judicial or administrative proceeding, or is otherwise requested or required to be disclosed by law or regulation, although the requirements of paragraph 4 hereof shall apply prior to any disclosure being made; and (e) is or has been independently developed by employees, consultants or agents of the Receiving Party without violation of the terms of this Agreement, as evidenced by the Receiving Party's records, and without reference or access to any Confidential Information.

2. **Disclosure of Confidential Information.**

From time to time, the Disclosing Party may disclose Confidential Information to the

Receiving Party. The Receiving Party will: (a) limit disclosure of any Confidential Information to its directors, officers, employees, agents or representatives (collectively "Representatives") who have a need to know such Confidential Information in connection with the current or contemplated business relationship between the parties to which this Agreement relates, and only for that purpose; (b) advise its Representatives of the proprietary nature of the Confidential Information and of the obligations set forth in this Agreement, require such Representatives to be bound by written confidentiality restrictions no less stringent than those contained herein, and assume full liability for acts or omissions by its Representatives that are inconsistent with its obligations under this Agreement; (c) keep all Confidential Information strictly confidential by using a reasonable degree of care, but not less than the degree of care used by it in safeguarding its own confidential information; and (d) not disclose any Confidential Information received by it to any third parties (except as otherwise provided for herein).

3. Use of Confidential Information.

The Receiving Party agrees to use the Confidential Information solely in connection with the current or contemplated business relationship between the parties and not for any purpose other than as authorized by this Agreement without the prior written consent of an authorized representative of the Disclosing Party. No other right or license, whether expressed or implied, in the Confidential Information is granted to the Receiving Party hereunder. Title to the Confidential Information will remain solely in the Disclosing Party. All use of Confidential Information by the Receiving Party shall be for the benefit of the Disclosing Party and any modifications and improvements thereof by the Receiving Party shall be the sole property of the Disclosing Party.

4. Compelled Disclosure of Confidential Information

Notwithstanding anything in the foregoing to the contrary, the Receiving Party may disclose Confidential Information pursuant to any governmental, judicial, or administrative order, subpoena, discovery request, regulatory request or similar method, provided that the Receiving Party promptly notifies, to the extent practicable, the Disclosing Party in writing of such demand for disclosure so that the Disclosing Party, at its sole expense, may seek to make such disclosure subject to a protective order or other appropriate remedy to preserve the confidentiality of the Confidential Information; provided **that the Receiving Party will disclose only that portion of the requested Confidential Information that, in the written opinion of its legal counsel, it is required to disclose**. The Receiving Party agrees that it shall not oppose and shall cooperate with efforts by, to the extent practicable, the Disclosing Party with respect to any such request for a protective order or other relief. Notwithstanding the foregoing, if the Disclosing Party is unable to obtain or does not seek a protective order and the Receiving Party is legally requested or required to disclose such Confidential Information, disclosure of such Confidential Information may be made without liability.

5. **Term**.

This Agreement shall remain in effect for a ………… year term (subject to a one-year extension if the parties are still discussing and considering the Transaction at the end of the second year). Notwithstanding the foregoing, the Receiving Party's duty to hold in confidence Confidential Information that was disclosed during term shall remain in effect indefinitely.

6. **Remedies**.

Both parties acknowledge that the Confidential Information to be disclosed hereunder is of a unique and valuable character, and that the unauthorized dissemination of the Confidential Information would destroy or diminish the value of such information. The damages to Disclosing Party that would result from the unauthorized dissemination of the Confidential Information would be impossible to calculate. Therefore, both parties hereby agree that the Disclosing Party shall be entitled to injunctive relief preventing the dissemination of any Confidential Information in violation of the terms hereof. Such injunctive relief shall be in addition to any other remedies available hereunder, whether at law or in equity. Disclosing Party shall be entitled to recover its costs and fees, including reasonable attorneys' fees, incurred in obtaining any such relief. Further, in the event of litigation relating to this Agreement, the prevailing party shall be entitled to recover its reasonable attorney's fees and expenses.

7. **Return of Confidential Information**.

Receiving Party shall immediately return and redeliver to Disclosing Party all tangible material embodying any Confidential Information provided hereunder and all notes, summaries, memoranda, drawings, manuals, records, excerpts or derivative information deriving therefrom, and all other documents or materials ("Notes") (and all copies of any of the foregoing, including "copies" that have been converted to computerized media in the form of image, data, word processing, or other types of files either manually or by image capture) based on or including any Confidential Information, in whatever form of storage or retrieval, upon the earlier of (i) the completion or termination of the dealings between the parties contemplated hereunder; (ii) the termination of this Agreement; or (iii) at such time as the Disclosing Party may so request; provided however that the Receiving Party may retain such of its documents as is necessary to enable it to comply with its reasonable document retention policies. Alternatively, the Receiving Party, with the written consent of the Disclosing Party may (or in the case of Notes, at the Receiving Party's option) immediately destroy any of the foregoing embodying Confidential Information (or the reasonably non-recoverable data erasure of computerized data) and, upon request, certify in writing such destruction by an authorized officer of the Receiving Party supervising the destruction).

8. **Notice of Breach**.

Receiving Party shall notify the Disclosing Party immediately upon discovery of, or suspicion of, (1) any unauthorized use or disclosure of Confidential Information by Receiving Party or its Representatives**; or (2) any actions by Receiving Party or its Representatives inconsistent with their respective obligations under** this Agreement, Receiving Party shall cooperate with any and all efforts of the Disclosing Party to help the Disclosing Party regain possession of Confidential Information and prevent its further unauthorized use.

9. **No Binding Agreement for Transaction**.

The parties agree that neither party will be under any legal obligation of any kind whatsoever with respect to a Transaction by virtue of this Agreement, except for the matters specifically agreed to herein. The parties further acknowledge and agree that they each reserve the right, in their sole and absolute discretion, to reject any and all proposals and to terminate discussions and negotiations with respect to a Transaction at any time. This Agreement does not create a joint venture or partnership between the parties. If a Transaction goes forward, the non-disclosure provisions of any applicable transaction documents entered into between the parties (or their respective affiliates) for the Transaction shall supersede this Agreement. In the event such provision is not provided for in said transaction documents, this Agreement shall control.

10. **Warranty**.

NO WARRANTIES ARE MADE BY EITHER PARTY UNDER THIS AGREEMENT WHATSOEVER. The parties acknowledge that although they shall each endeavour to include in the Confidential Information all information that they each believe relevant for the purpose of the evaluation of a Transaction, the parties understand that no representation or warranty as to the accuracy or completeness of the Confidential Information is being made by the Disclosing Party. Further, neither party is under any obligation under this Agreement to disclose any Confidential Information it chooses not to disclose.

11. **Miscellaneous**.

(a) This Agreement constitutes the entire understanding between the parties and supersedes any and all prior or contemporaneous understandings and agreements, whether oral or written, between the parties, with respect to the subject matter hereof. This Agreement can only be modified by a written amendment signed by the party against whom enforcement of such modification is sought.

(b) The validity, construction and performance of this Agreement shall be governed and construed in accordance with the laws of _____________________ (state) applicable to contracts made and to be wholly performed within such state, without giving effect to any conflict of law's provisions thereof. The Federal and state courts located in _______________ (state) shall have sole and exclusive jurisdiction over any disputes arising under**, or in any way connected with or related to,** the terms of this Agreement **and Receiving Party: (i) consents to personal jurisdiction therein; and (ii) waives the right to raise *forum non conveniens* or any similar objection.**

(c) Any failure by either party to enforce the other party's strict performance of any provision of this Agreement will not constitute a waiver of its right to subsequently enforce such provision or any other provision of this Agreement.

(d) Although the restrictions contained in this Agreement are considered by the parties to be reasonable for the purpose of protecting the Confidential Information, if any such restriction is found by a court of competent jurisdiction to be unenforceable, such provision will be modified, rewritten or interpreted to include as much of its nature and scope as will render it enforceable. If it cannot be so modified, rewritten or interpreted to be enforceable in any respect, it will not be given effect, and the remainder of the Agreement will be enforced as if such provision was not included.

(e) Any notices or communications required or permitted to be given hereunder may be delivered by hand, deposited with a nationally recognized overnight carrier, electronic-mail, or mailed by certified mail, return receipt requested, postage prepaid, in each case, to the address of the other party first indicated above (or such other addressee as may be furnished by a party in accordance with this paragraph). All such notices or communications shall be deemed to have been given and received (a) in the case of personal delivery or electronic-mail, on the date of such delivery, (b) in the case of delivery by a nationally recognized overnight carrier, on the third business day following dispatch and (c) in the case of mailing, on the seventh business day following such mailing.

(f) This Agreement is personal in nature, and neither party may directly or indirectly assign or transfer it by operation of law or otherwise without the prior written consent of the other party, which consent will not be unreasonably withheld. All obligations contained in this Agreement shall extend to and be binding upon the parties to this Agreement and their respective successors, assigns and designees.

(g) The receipt of Confidential Information pursuant to this Agreement will not prevent or in any way limit either party from: (i) developing, making or marketing products or services that are or may be competitive with the products or services of the other; or (ii) providing products or services to others who compete with the other.

(h) Paragraph headings used in this Agreement are for reference only and shall not be used or relied upon in the interpretation of this Agreement.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date first above written.

Disclosing Party	**Receiving Party**
By________________________	By ______________________
Name:	Name:
Title:	Title: