

PRIVACY POLICY

North East Transmission Company Limited (NETC)

Effective Date: 11.09.2026

1. Introduction

North East Transmission Company Limited (“NETC”, “Company”, “we”, “our” or “us”) is committed to protecting the privacy and security of information processed through its mobile application (“Application”).

This Privacy Policy describes the manner in which information may be collected, used, stored, processed and protected when an authorized user accesses or uses the NETC NETRA Application.

The NETC NETRA application is intended primarily for authorized users and for official purposes connected with NETC’s operations and activities.

NETC’s Information Security Policy establishes requirements for protection of Information Assets and for maintaining confidentiality, integrity, availability and accountability of organizational information.

2. Information That May Be Collected

Depending upon the functionality and permissions of the Application, NETC may collect and process the following categories of information:

2.1 User Information

- Name;
- Employee or user identification details;
- Official designation;
- Department or office;
- Official contact details;
- User account and authentication-related information.

2.2 Operational Information

The Application may collect information submitted by users during the performance of authorized official activities, including:

- Inspection or patrolling records;
- Observations and reports;
- Dates and time of activities;
- Equipment, asset or location references;
- Other information required for official operational purposes.

2.3 Location Information

Where required for Application functionality, the Application may collect location information, including GPS coordinates, during authorized use of the Application.

Location information may be used for verification, monitoring, reporting, operational planning and other legitimate official purposes.

2.4 Photographs and Media

Where enabled and required for official functionality, the Application may access the device camera or receive photographs and other media submitted by users.

Such information may be used as supporting evidence or records relating to authorized official activities.

2.5 Technical and Security Information

The Application and its associated systems may automatically generate technical and security-related information, including:

- Login and logout information;
- Date and time of access;
- Device or Application-related information;
- IP address or network-related information, where applicable;
- System and Application logs;
- Error and diagnostic information; and
- Security and audit trail information.

3. Purpose of Collection and Use

Information collected through the Application may be used for the following purposes:

- a. To authenticate and authorize users;
- b. To provide the intended functionality of the Application;
- c. To facilitate authorized official and operational activities;
- d. To record, verify and monitor official activities;
- e. To maintain operational records and reports;
- f. To improve the performance, security and reliability of the Application;
- g. To investigate technical problems, misuse or security incidents;
- h. To comply with applicable legal, regulatory, audit and organizational requirements; and
- i. For other legitimate purposes connected with NETC's authorized operations.

Information shall not be used for purposes inconsistent with the legitimate and authorized functions of the Application.

4. Location and Camera Permissions

The Application may request permission to access the location services and camera of the user's device where such access is necessary for the intended official functionality of the Application.

Location and camera permissions shall be used only for the functions for which such permissions are required.

Users may manage certain permissions through their device settings. However, disabling necessary permissions may affect the availability or functioning of certain Application features.

5. Information Security

NETC shall implement reasonable administrative, technical and organizational measures to protect information processed through the Application against unauthorized access, alteration, loss, misuse or disclosure.

NETC's Information Security Policy requires protection of Information Assets, prevention of unauthorized access and implementation of Information Security controls.

Appropriate access controls and security measures may be implemented based on the nature and sensitivity of the information and the operational requirements of the Application.

6. Access to Information

Access to information collected or processed through the Application shall be restricted to authorized personnel, users or service providers who require such access for legitimate and authorized purposes.

Access permissions may be based on the user's role, responsibilities and operational requirements.

NETC may review and modify user access rights whenever required for security, operational or administrative purposes.

7. Sharing and Disclosure of Information

NETC may share or disclose information only where necessary and authorized, including:

- a. With authorized NETC officials and departments;
- b. With authorized service providers engaged for operation, maintenance or support of the Application, subject to applicable contractual and confidentiality requirements;
- c. With competent governmental, regulatory, statutory or law-enforcement authorities where required under applicable law; and

- d. Where disclosure is otherwise necessary for protection of NETC's legitimate interests, Information Assets or security.

NETC shall not knowingly disclose official or confidential information for unauthorized purposes.

8. Data Storage and Retention

Information collected through the Application shall be retained for the period required for official, operational, legal, regulatory, audit and record-management purposes.

The retention period may vary depending upon:

- The nature of the information;
- Operational requirements;
- Applicable legal or regulatory requirements;
- Audit and investigation requirements; and
- NETC's applicable record retention policies.

Security and system logs may be retained in accordance with NETC's applicable Information Security requirements. The NETC policy provides for secure retention of relevant system, security, firewall and VPN logs for a minimum period of one year for covered systems.

9. Data Accuracy

Users are responsible for ensuring that information submitted through the Application is accurate and genuine.

Where the Application permits correction or modification of submitted information, such changes shall be subject to the applicable authorization and audit controls.

NETC may retain records or audit trails of information submitted, modified or processed through the Application for security, audit and operational purposes.

10. Security Monitoring and Audit Logs

NETC may maintain system logs, audit trails and other records relating to access and use of the Application.

Such information may include records of:

- User access;
- Activities performed through the Application;
- System events;
- Errors and technical events; and
- Security-related events.

Such records may be used for system administration, security monitoring, incident investigation, audit, compliance and protection of NETC's Information Assets.

11. Security Incidents

In the event of a suspected or actual security incident affecting information processed through the Application, NETC may take appropriate actions to investigate, contain, mitigate and respond to the incident.

Users shall promptly report suspected security incidents, unauthorized access, compromise of credentials or loss of devices containing official Application information to the concerned NETC authority/IT Department.

NETC's Information Security Policy requires immediate reporting of security incidents and establishes an organizational escalation mechanism for such incidents.

12. Third-Party Services

Where the Application uses third-party infrastructure, services, software components or support services, such services may process information strictly to the extent necessary for providing the Application functionality or associated technical support.

NETC shall endeavor to ensure that authorized third-party service providers handling NETC information are subject to appropriate contractual, confidentiality and security obligations, as applicable.

13. User Responsibilities

Users shall:

- Use the Application only for authorized purposes;
- Keep authentication credentials confidential;
- Protect the device used for accessing the Application;
- Avoid unauthorized sharing or disclosure of official information;
- Promptly report suspected security incidents;
- Comply with applicable NETC policies and instructions.

Users are responsible for activities performed through their accounts, as recognized under NETC's Information Security Policy.

14. Changes to this Privacy Policy

NETC may amend or update this Privacy Policy from time to time to reflect changes in:

- Application functionality;
- Operational requirements;
- Information Security requirements;
- Applicable laws or regulations; or
- Organizational policies.

The revised Privacy Policy may be made available through the Application or other appropriate official channels.

15. Contact and Grievance/Privacy Queries

For questions, concerns or requests relating to this Privacy Policy or the processing of information through the Application, users may contact:

North East Transmission Company Limited (NETC)
IT Department / Authorized Officer

Email: it@netcindia.in

Telephone: 8811072489

16. Acceptance

By downloading, accessing or using the Application, the user acknowledges that he/she has read and understood this Privacy Policy and agrees to the processing of information as described herein, subject to applicable laws and NETC's authorized operational requirements.