Steelman Telecom Limited

(Formerly known as Steelman Telecom Private Limited)

DATA PROTECTION AND INFORMATION SECURITY POLICY

Steelman Telecom Limited

1. Introduction and Purpose

Steelman Telecom Limited ("Steelman") is committed to protecting the personal data and confidential information of our clients, employees, and stakeholders in accordance with applicable data protection laws and contractual obligations. This policy establishes the framework for how Steelman handles, processes, stores, and protects personal data and sensitive information across all business operations, particularly in relation to service delivery contracts such as those with Client Solutions and Networks.

The objective of this policy is to:

- Ensure compliance with applicable data protection regulations and contractual requirements;
- Protect the confidentiality, integrity and availability of personal data;
- Establish clear roles, responsibilities and procedures for all personnel;
- Manage security risks and respond to incidents promptly;
- Maintain appropriate records and documentation.

2. Scope and Applicability

This policy applies to:

- All Steelman employees, contractors, and representatives involved in processing personal data or accessing client systems;
- All systems, applications, databases, storage media (including NAS, servers, laptops, mobile devices) and facilities used to process, store or transmit personal data;
- All projects and engagements where personal data is handled, including projects and similar client contracts.

This policy does not apply to:

- Publicly available, aggregated, or anonymized data that cannot identify individuals;
- Data handled by third-party service providers outside Steelman's control (though we remain accountable for their compliance where contractually required).

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

3. Roles and Responsibilities

3.1 Management and Leadership

Senior management is responsible for:

- Ensuring adequate resources and budget for data protection and information security.
- Approving updates to this policy and related procedures.
- Ensuring compliance with legal and contractual obligations.
- Supporting a culture of security and confidentiality across the organization.

3.2 Data Protection Officer / Compliance Lead

Steelman designates a Data Protection Officer or nominated compliance lead who is responsible for:

- Coordinating data protection and security initiatives;
- Serving as the point of contact for client data protection representatives.
- Monitoring compliance with this policy and data handling procedures;
- Investigating and reporting security incidents;
- Ensuring training and awareness programs are in place;
- Maintaining records of processing activities and risk assessments.

3.3 All Personnel

Every employee and contractor must:

- Read and understand this policy;
- Complete mandatory data protection and security training annually or upon hire;
- Follow all procedures for handling personal data and confidential information;
- Report any suspected security incident, policy breach or data misuse to management immediately;
- Use personal data only as authorized for their role and project;
- Keep passwords and authentication credentials confidential;
- Comply with all remote access and security requirements.

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

4. Data Classification and Handling

4.1 Data Classification Framework

Personal data processed by Steelman is classified into the following categories:

Confidential (Client) Personal Data:

Data provided by clients that is explicitly marked as confidential or contains sensitive information about individuals (e.g. names, contact details, network identifiers, location data, performance metrics). This data must be protected with the highest level of access controls and encryption.

Internal Employee Data:

Personal data of Steelman employees (e.g. names, addresses, salary, performance records). This data is used only for HR, payroll and management purposes and is protected with role-based access control.

General Business Information:
Non-confidential business data, operational information and internally-generated reports. This data may be shared internally as needed for business operations.

4.2 Data Handling Standards

Data Storage and Management for Confidential (Client) Personal Data:

- Access personal data only on a need-to-know basis for their assigned role or project;
- Never share personal data via email unless explicitly encrypted or approved by the data protection lead;
- Not copy, download or remove personal data from designated systems without prior authorization;
- Apply appropriate encryption when transferring data (minimum 128-bit encryption);
- Store personal data only on approved company systems (e.g. company NAS, secured servers, encrypted devices);
- Never store personal data on personal devices, portable media or cloud storage without explicit written approval;
- Immediately report any suspected loss, theft or unauthorized access to personal data;
- Comply with data retention and deletion instructions from clients (see Section 5 below).

Certified to be a true copy

Steelman Telecom Limited * Kolkata *

Data Storage and Management for Internal Employee Data:

- **HR, IT and Purchase Order (PO) data:** Stored only in Steelman's own portal "ESTL", which is hosted on secured AWS and local servers under IT control. Access to
- this portal is restricted to authorized HR and management personnel on a need-to-know basis.
- **Financial and invoice records:** All invoices and related financial documents are stored in the Tally cloud environment. Archival copies for disaster recovery purposes are maintained on Steelman-managed NAS devices with restricted access controls.
- **Backup retrieval and cloud exports:** Any backup retrieval or export from cloud systems (ESTL, Tally, or related platforms) requires prior written email approval from the relevant function owner:
    - **HR data:** Requires approval from the HR team;
    - **Purchase orders and vendor data:** Requires approval from the CFO or PO team;
    - **Financial documents and accounting records:** Requires approval from the Accounts team;
    - All such approvals are retained in the Office 365 email system where they are immutable and cannot be modified or deleted by end users, providing an audit trail for all data exports and backups.
- **Disaster recovery archival:** All employee data requiring archival is backed up to NAS devices for disaster recovery purposes. These archival copies are retained according to Section 5.1 retention periods and are subject to the same deletion and return procedures as client data.

4.3 Clean Desk and Facility Security

- Printed documents containing personal data must not be left unattended on desks or in common areas;
- Sensitive documents must be stored in locked drawers or cabinets;
- Computer screens must be locked when unattended or sessions logged out after 15 minutes of inactivity;
- Personal data must not be discussed in public areas or overheard by unauthorized individuals;
- Visitors to facilities where personal data is processed must be escorted and registered.

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

5. Data Retention, Deletion and Return

5.1 Retention Periods

Personal data will be retained only for as long as necessary to deliver the contracted services and meet legal or contractual obligations. Specific retention periods are:

- **Client project data:** Retained until the project is completed and the client confirms no further data is needed. Default retention is the contract period plus any agreed handover period.
- **Statutory financial and accounting records:** Maintained for a minimum of eight (8) financial years in line with applicable Indian company and tax law requirements, or longer where any regulator or legal proceeding requires extended retention.
- **Telecom operational records (e.g., CDRs, subscriber/KYC data):** Retained in accordance with applicable DoT/TRAI license conditions and law-enforcement requirements. Typical retention ranges from one (1) year for certain call or network logs to several years for subscriber and KYC records, depending on the record type and legal obligations.
- **Employee data:** Retained for the duration of employment plus legally required periods (typically 3–7 years depending on local law).
- **Backup and archival copies (including NAS backups):** Retained only as part of normal backup cycles on Steelman-managed NAS and backup systems and, once data is flagged for deletion or a project end, kept for no longer than 10 years, after which the backups are automatically overwritten or securely destroyed.

5.2 Data Deletion and Disposal

Upon the completion or termination of a project, or upon client instruction:

1. Steelman will securely delete or return all personal data in its possession to the client, unless the client has instructed otherwise;
2. Deletion will be performed using industry-standard secure deletion methods to ensure data cannot be recovered;
3. Deletion will be documented with evidence (e.g., certificate of deletion, dated records) provided to the client on request;
4. Backup copies held on NAS or in archival systems will be allowed to remain until the normal backup retention cycle (maximum 6 months) elapses, after which they are overwritten as part of routine maintenance;
5. Any media or devices that are no longer needed will be physically destroyed or securely wiped prior to disposal.

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

5.3 Data Return Process

When a client requests the return of personal data:

1. The data protection lead will coordinate with the project team to identify all locations where the data is stored (e.g., project servers, NAS, employee workstations, backups);
2. Data will be packaged in a secure format (encrypted transfer or physical media with encryption);
3. A receipt or delivery confirmation will be obtained from the client;
4. Internal systems will be marked to indicate that the data has been returned.

6. Access Control and User Management

6.1 User Access Provisioning

- All user accounts are created only upon formal request and are assigned the minimum privileges necessary to perform the assigned role (least privilege principle);
- Individual user accounts are assigned to each person; shared accounts are prohibited;
- Accounts are granted access to specific systems, databases, networks and client environments only as needed;
- Access is documented and reviewed quarterly by management.

6.2 User Account Management

- Passwords must be strong (minimum 12 characters, upper/lowercase letters, numbers and special characters) and changed every 90 days;
- Multi-factor authentication (MFA) is required for any remote access to client systems or sensitive company systems;
- Admin or privileged access is granted only to trained personnel and is reviewed annually;
- User accounts must be disabled immediately upon termination or role change;
- Inactive accounts are reviewed quarterly and disabled after 60 days of no activity.

6.3 Physical Access Control

- Steelman offices and IT facilities are secured with locked doors, key card access or biometric controls;
- Only authorized employees have access to areas where personal data is stored or processed;

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

- All personnel are required to carry and display identification badges;
- Visitors are registered upon entry, escorted at all times and required to sign confidentiality agreements;
- Access logs are maintained and reviewed periodically;
- After-hours access is monitored and recorded.

7. Network and System Security

7.1 Network Infrastructure

Steelman's network protecting personal data includes:

- **Firewalls:** Deployed at network perimeters to monitor and control traffic based on access control lists (ACLs). All inbound and outbound traffic is logged.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Monitor network traffic for suspicious patterns and malicious activity.
- **Virtual Private Networks (VPN):** Remote access to company or client systems is only via approved VPN servers with minimum 128-bit encryption, two-factor authentication, and split tunneling disabled.
- **Anti-spoofing filters:** Enabled on all network devices to prevent IP spoofing attacks.
- **Email security:** Transport Layer Security (TLS) is enabled for email communication between Steelman and client domains. Non-company email access from company devices is disabled unless explicitly approved by clients.

7.2 Endpoint and Device Security

All laptops, desktops and mobile devices used to access personal data or client systems must:

- Have operating system and security patches applied automatically or within 30 days of release;
- Use full-disk encryption (minimum 256-bit AES) to protect data if the device is lost or stolen;
- Have anti-malware and antivirus software installed and updated;
- Enforce strong authentication (password or PIN, minimum 12 characters);
- Auto-lock after 15 minutes of inactivity;
- Have remote wipe capability enabled for mobile devices;
- Prohibit installation of unauthorized software or modification of security settings by users.

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

7.3 Vulnerability Management

- Steelman conducts vulnerability scans of network devices and systems quarterly or upon notification of a known vulnerability;
- High-risk vulnerabilities are patched within 30 days; critical vulnerabilities are patched within 7 days;
- Penetration testing or security assessments are conducted annually;
- Remediation efforts are documented and tracked.

7.4 Data Encryption

- Personal data in transit is encrypted using a minimum of 128-bit encryption (e.g., AES, TLS);
- Personal data at rest on company systems (NAS, servers, databases) is encrypted using a minimum of 256-bit encryption;
- Encryption keys are managed securely and never shared in plain text;
- Where data must be transferred to or from clients, encryption is mandatory unless explicitly waived by the client.

8. Logging, Monitoring and Incident Management

8.1 System and Application Logging

Systems and applications used to process personal data maintain detailed logs of:

- User login/logout activities;
- All access to personal data (view, modify, delete);
- Administrative actions (account creation/deletion, permission changes);
- System configuration changes;
- Failed access attempts;
- Errors and exceptions.

Logs are retained for a minimum of 90 days and are reviewed regularly for anomalies or suspicious activity.

8.2 Security Monitoring

- Steelman maintains continuous or frequent monitoring of systems processing personal data;
- Alerts are configured for suspicious activities (e.g., multiple failed login attempts, after-hours access, bulk data downloads);

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

- Monitoring logs and alerts are reviewed daily or as part of automated security processes;
- Any suspicious activity is investigated promptly and reported to management.

8.3 Incident Detection and Response

8.3.1 Incident Definition

A security incident includes:

- Unauthorized access to or disclosure of personal data;
- Loss, theft or misplacement of devices or media containing personal data;
- Suspected malware infection or system compromise;
- Accidental deletion or corruption of personal data;
- Failure of security controls or systems;
- Any suspected breach of this policy or data protection requirements.

8.3.2 Reporting Obligations

Any employee who suspects a security incident must:

- Immediately notify their manager and the data protection lead (do not attempt to investigate independently);
- Provide details of what was observed, when it occurred, what systems or data may be affected, and any immediate actions taken;
- Preserve evidence (e.g., log files, screenshots) without altering systems unless necessary for containment.

8.3.3 Incident Response Process

Upon notification of a suspected incident, Steelman will:

1. **Contain:** Immediately isolate affected systems if necessary to prevent further unauthorized access or data loss;
2. **Investigate:** Determine the scope of the incident, affected data and individuals, root cause, and whether external parties (e.g., attackers) were involved;
3. **Document:** Record all findings, timeline, actions taken and evidence gathered;
4. **Remediate:** Close the security gap or restore systems to a secure state;
5. **Notify:** Inform affected clients without undue delay if their personal data has been compromised; notify individuals affected if legally required;

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

6. **Review:** Conduct a post-incident review to identify lessons learned and prevent recurrence.

8.3.4 Incident Escalation Timeline

- **Initial detection/reporting:** Within 24 hours of discovery;
- **Client notification:** Without undue delay and in accordance with contractual obligations (typically within 72 hours for serious incidents);
- **Regulatory notification:** In accordance with applicable data protection law (e.g., GDPR, India's DPDP Act).

8.4 Incident Register

Steelman maintains a confidential incident register documenting:

- Date and time of discovery;
- Description of the incident;
- Systems and data affected;
- Response actions taken;
- Outcome and lessons learned;
- Follow-up actions to prevent recurrence.

9. Training and Awareness

9.1 Mandatory Training

All Steelman employees and contractors must complete:

- **Initial data protection training** upon hire or project start, covering:
    - This policy and key responsibilities;
    - Confidentiality and data handling rules;
    - Incident reporting procedures;
    - Password and authentication best practices;
    - Clean desk and physical security.
- **Annual refresher training** to maintain awareness and comply with client requirements;
- **Role-specific training** for personnel with elevated access or data handling responsibilities (e.g., administrators, developers, compliance staff), covering:

Certified to be a true copy

Steelman Telecom Limited Kolkata

- Advanced security controls and access management;
- Vulnerability management and patching;
- Incident response procedures;
- Compliance requirements specific to their role.

- **Client-specific training** when required by clients (e.g. data protection training), to be completed before accessing client systems or data.

9.2 Training Records

Training completion is tracked and documented. Failure to complete mandatory training may result in:

- Suspension of system or project access until training is completed;
- Performance management action;
- Disciplinary action for policy breaches.

9.3 Security Awareness Communications

Steelman periodically distributes security awareness communications covering:

- Phishing and social engineering threats;
- Password hygiene and multi-factor authentication;
- Ransomware and malware prevention;
- Data handling best practices;
- Recent security incidents or threats and how to respond.

10. Compliance and Audit

10.1 Policy Compliance Reviews

- Steelman's data protection lead will conduct quarterly compliance reviews to assess adherence to this policy and identify gaps;
- Management will review incident trends, training completion rates and access control effectiveness;
- Findings will be documented and shared with senior management.

10.2 Internal Audits

- Annual internal audits will assess the effectiveness of data protection controls, including network security, access management, logging and incident response;
- Audit findings and corrective actions will be documented and tracked;

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

- Management will prioritize remediation of high-risk findings.

10.3 External Audits and Certifications

Steelman is committed to pursuing or maintaining industry-recognized security certifications or assessments where contractually required or operationally beneficial (e.g., ISO 27001, SOC 2 Type II compliance). Such certifications demonstrate adherence to international data protection and security standards.

10.4 Client Audits and Assessments

Steelman cooperates fully with client audits, security assessments and inspections related to data protection and compliance. Clients have the right to:

- Request documentation of security controls and procedures;
- Conduct on-site audits or security assessments;
- Review logs and incident records;
- Request evidence of staff training and awareness.

11. Legal and Regulatory Compliance

11.1 Applicable Laws

Steelman acknowledges and commits to comply with all applicable data protection and privacy laws in jurisdictions where it operates, including but not limited to:

- India's Digital Personal Data Protection Act, 2023 (DPDP Act);
- General Data Protection Regulation (GDPR) to the extent applicable to EU data subjects or clients;
- Any data protection law applicable to clients' territories or operations.

11.2 Data Subject Rights

Where applicable law grants rights to individuals (data subjects) whose personal data is processed by Steelman:

- Steelman will honor requests to access, correct, delete or port personal data, subject to contractual restrictions.
- Requests will be directed to the appropriate client or Steelman's data protection lead, who will coordinate a response within legally required timeframes;
- Steelman will not unreasonably delay or refuse such requests.

Certified to be
a true copy

Steelman Telecom Limited
Kolkata

11.3 Contractual Compliance

Steelman ensures that contracts with clients include:

- Clear definition of the personal data being processed;
- Specification of the purposes and lawful basis for processing;
- Description of data protection and security measures;
- Data retention and deletion terms;
- Incident notification procedures;
- Data subject rights and procedures;
- Allocation of responsibilities between Steelman and the client.

12. Consequences of Policy Breach

12.1 Disciplinary Action

Any violation of this policy by Steelman personnel may result in disciplinary action, including:

- Verbal or written warning;
- Suspension of system or project access;
- Mandatory retraining;
- Performance improvement plan;
- Demotion or reassignment;
- Termination of employment.

The severity of disciplinary action depends on the nature, scope and intent of the breach, and whether it resulted in actual harm or regulatory penalty.

12.2 Contractual Consequences

Breaches of this policy that result in client data compromise, compliance violations or regulatory penalties may expose Steelman to:

- Contractual penalties or liability;
- Loss of client projects or contracts;
- Regulatory fines or enforcement action;
- Reputational damage.

13. Policy Review and Updates

13.1 Regular Review

This policy will be reviewed annually or sooner if:

Steelman Telecom Limited Kolkata

Certified to be a true copy

- Significant security incidents or breaches occur;
- Applicable laws or regulations change;
- Client requirements or best practices evolve;
- Technology or business operations change substantially;
- Audits or assessments identify gaps.

13.2 Version Control and Communication

Updates to this policy will be:

- Documented with a new version number and effective date;
- Communicated to all personnel;
- Incorporated into mandatory training and awareness programs;
- Provided to clients and subcontractors as appropriate.

14. Contact Information

Data Protection Officer / Compliance Lead:

Name: PRATAP MAITY
Position: IT HEAD
Email: PRATAP.MAITY@STEELMANTELECOM.COM
Phone: 8436821992

For policy questions, compliance concerns or to report a security incident, please contact the Data Protection Officer.

15. LIMITATION, REVIEW AND AMENDMENT:

In the event of any conflict between the provisions of this Policy and of the Act or the Listing Regulations or any other legal requirement ("Applicable Law"), the provisions of Applicable Law shall prevail over this Policy. Any subsequent amendment / modification to the Applicable Law shall automatically apply to this Policy.

The Board may review this Policy periodically (and at least once every three years) and make amendments from time to time, as may be deemed necessary (including based on recommendation(s) of the Audit Committee).

****

FOR STEELMAN TELECOM LIMITED

Steelman Telecom Limited

Director

MAHENDRA BINDAL
MANAGING DIRECTOR
DIN: 00484964

Certified to be a true copy

Steelman Telecom Limited Kolkata