

# **Data Protection and Privacy Policy**

## **1. Purpose**

At Antier Solutions, we prioritize the security, confidentiality, and lawful handling of all data associated with our employees, clients, partners, and internal business operations. The purpose of this policy is to establish a robust framework for the collection, processing, storage, sharing, and disposal of data, and to ensure that every stakeholder understands their role in maintaining data integrity and privacy.

We aim to:

* Ensure compliance with applicable laws and regulations such as the IT Act, GDPR (where applicable), and client contractual obligations.
* Prevent unauthorized access, loss, theft, misuse, or disclosure of sensitive data.
* Promote a culture of accountability and responsibility when handling digital and physical data.

## **2. Scope**

This policy applies to:

* All employees, interns, consultants, freelancers, contractors, vendors, and any third-party service providers working with Antier Solutions.
* All data is processed through our internal systems, client-facing platforms, servers, mobile devices, emails, documents, or software tools.
* Both on-premise and remote work environments (including Work From Home arrangements).

## **3. Definitions**

* **Personal Data**: Any data that can identify an individual (e.g., name, ID proof, contact information, medical records).
* **Confidential Business Information**: Company strategies, financial reports, source codes, blueprints, proprietary models.
* **Client Data**: Information shared by clients such as project codes, NDAs, business requirements, and customer databases.
* **Sensitive Data**: Includes passwords, financial credentials, biometric info, and trade secrets.

## **4. Data Collection and Usage**

### **a. What We Collect:**

* **Employee Information**: Name, address, Aadhar/PAN, contact details, educational records, banking details, emergency contacts, etc. (Collected on the day of joining)
* **Client Information**: Project scope, software architecture, user databases, API credentials, legal contracts.
* **System Information**: Email logs, system access logs, attendance data, CCTV footage, asset use logs.

### **b. Why We Collect:**

* For regulatory and compliance needs.
* For payroll and benefits administration.
* For project execution and client obligations.
* For monitoring, safety, and operational efficiency.

## **5. Access Control and Authorization**

* Access to sensitive and confidential information is provided strictly on a **need-to-know** and **least privilege** basis.
* Department heads and IT control access rights through role-based authorization systems (RBAC).
* Unauthorized sharing, copying, storing, or transmitting company or client data via external devices, cloud storage, personal email, or drives is **strictly prohibited**.

## **6. Data Storage, Backup & Retention**

* All data is stored securely using industry-grade encrypted servers (internal or cloud-based, as approved).
* Regular data backups are conducted, and business continuity measures are in place.
* Data retention periods vary based on the requirement
* Upon resignation, termination, or contract completion, all access is revoked, and data must be returned or deleted.

## **7. Data Transfer & External Communication**

* No employee is allowed to send sensitive data via personal accounts or unauthorized platforms.
* Data transfers (internally or externally) must be encrypted, monitored, and logged.
* Any sharing with third parties must be pre-approved by department heads and legal/HR teams and supported by a **signed NDA**.

## **8. Responsibilities of Employees**

* Follow the principle of **data minimization**: only collect, store, or share what is strictly necessary.
* Lock devices when away from the desk, especially when handling sensitive data.
* Report suspicious activity, unauthorized access, or data loss to **IT and HR immediately**.
* Never speak about sensitive client or company matters in public, on social media, or through unsecured platforms.

## **9. Use of Devices and Systems**

* Only company-authorized devices and networks should be used for official work in exceptional cases where HR or an authorized person allows or asks to use a personal system.
* Installation of any unauthorized software, tools, or extensions is **strictly forbidden**.
* All emails, chats, and file sharing must be done through approved company platforms (e.g., Outlook, Slack, Zoom, Jira).

## **10. Data Breach Protocol**

In case of a suspected or confirmed data breach:

1. **Immediate Reporting**: Notify IT Security and HR at ithelpdesk@antiersolutions.com and hr@antiersolutions.com.
2. **Containment & Investigation**: IT will take steps to isolate and assess the breach.
3. **Impact Assessment**: Identify what data was affected, potential misuse, and risks.
4. **Mitigation & Notification**: Inform relevant stakeholders, including clients, and execute damage control.
5. **Corrective Action**: Include policy updates, retraining, or technical improvements.

## **11. Disciplinary Measures**

Violation of this policy is treated with **zero tolerance** and may result in:

* Immediate access revocation
* Formal warnings or a show-cause notice
* Suspension or termination of employment
* Legal proceedings, especially in case of:  
  + Data theft
  + Unauthorized sharing of client IP
  + Misuse of confidential files
  + Refusal to return company data upon exit

## **12. Training & Awareness**

* All employees will receive mandatory training on data security, privacy practices, and handling confidential information.
* Specialized training will be provided to teams handling large data volumes

## **13. Policy Enforcement & Audit**

* Regular audits will be conducted to ensure compliance with data protection protocols.
* Any lapse found during audits will be flagged to management, and necessary action will be taken.
* The policy will be reviewed biannually or as required to keep up with legal and technological changes.

## **14. Related Policies**

Employees must also refer to:

* Intellectual Property Rights Policy
* Code of Conduct
* IT & Asset Usage Policy
* Zero Tolerance Policy
* Exit and F&F Policy

## **Contact for Clarifications or Reporting:**

📧 **HR Department**: hr@antiersolutions.com  
 📧 **IT Security Team**: ithelpdesk@antiersolutions.com