Information Security and Asset Management Policy

# Purpose

This Information Security and Asset Management Policy establishes guidelines to protect Antier Solutions’ information assets, ensure the confidentiality, integrity, and availability (CIA) of data, and manage company assets responsibly. It aims to facilitate business improvement through secure practices, provide a strong commitment to information security, and support our mission of delivering innovative blockchain and tech solutions while maintaining a secure and compliant environment.

# Scope

This policy applies to all employees, contractors, vendors, and third parties who interact with Antier Solutions’ information systems, networks, devices, data, and physical assets, whether on-site, remotely, or via personal devices. It covers all IT resources, including hardware, software, networks, data, code repositories, and physical assets related to blockchain development, AI, and other emerging technologies.

# Definitions

* **Information Assets**: All data, systems, networks, and devices owned or managed by Antier Solutions.
* **Sensitive Data**: Confidential or proprietary information, including client data, intellectual property, blockchain smart contracts, and employee personal information.
* **Production Code**: Any code used in Antier Solutions’ live products, services, or client deliverables.
* **Official Repository**: A company-managed code repository hosted on a secure platform (e.g., GitHub, GitLab) under Antier Solutions’ official account.
* **BYOD (Bring Your Own Device)**: The use of personal devices to access company IT resources.
* **Shadow IT**: Unauthorized use of unapproved applications, devices, or services for company tasks.

# Information Security Management

## Objectives

* + - Ensure the **Confidentiality, Integrity, and Availability (CIA)** of information assets by implementing robust security controls.
    - Facilitate business improvement through the adoption of secure and innovative practices, particularly in blockchain and emerging tech development.
    - Demonstrate a strong commitment to information security by orienting and training all members of the organization.

## Ownership and Access

* + - Antier Solutions owns the rights to all data and files in any computer, network, or information system used by the company, as well as data sent or received using company systems or company-provided internet access, unless superseded by applicable intellectual property laws.
    - Employees have **no expectation of privacy** when using company systems, including electronic mail (e.g., personal, private, or instant messaging systems), internet access, and computer files.
    - The company reserves the right to monitor, view, download, inspect, release, and archive electronic mail messages, internet activity, and files stored on company systems at any time.
    - No employee may access another employee’s computer, files, or email without prior authorization from the employee or an appropriate company official (e.g., IT manager or HR).

## Monitoring and Logging

* + - Antier Solutions uses software to monitor and store copies of all messages, files, and activities on company systems, including emails, internet usage, and file access.
    - Employees should assume that all activities (e.g., emails sent/received, files accessed, internet browsing) are logged, stored, and subject to inspection by authorized personnel.
    - Employees waive any confidentiality or disclosure privileges when using company systems to send or receive privileged data, unless using non-company systems for such communications.

# Code Repository Management Policy

## Official Repository Requirement

* + - All production code must be stored exclusively in Antier Solutions’ official repositories, hosted on a secure platform (e.g., GitHub, GitLab) under the company’s official account.
    - The use of personal repository accounts (e.g., personal GitHub accounts) for storing, managing, or sharing production code is strictly prohibited.

## Code Publishing Restrictions

* + - Employees are prohibited from publishing production code, or any part of it, to public repositories, personal accounts, or external platforms without explicit written approval from the IT and legal teams.
    - Unauthorized publishing of code may lead to intellectual property breaches and will result in immediate disciplinary action, up to and including termination.

## Repository Privacy

* + - All product repositories must be set to private visibility to prevent unauthorized access to Antier Solutions’ intellectual property, including blockchain smart contracts, AI models, and client deliverables.
    - Access to repositories will be granted on a need-to-know basis, managed through role-based access controls, with permissions reviewed quarterly by the IT team.

## Code Review and Auditing

* + - All code commits to official repositories must undergo a mandatory peer review process to ensure quality, security, and compliance with Antier Solutions’ standards.
    - The IT team will conduct regular audits of repositories to ensure compliance with this policy, including verifying that no production code is stored in unauthorized locations.

# Email Policy

## Acceptable Use

* + - The official email system is for business purposes and must not be used for disruptive or offensive messages, including comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs, political beliefs, or national origin.
    - Employees who receive offensive emails must report them to their supervisor immediately.

## Email Security Guidelines

* + - **NEVER** open files or macros attached to emails from unknown, suspicious, or untrustworthy sources. Delete such attachments immediately and empty your Trash.
    - Delete spam, chain, and junk emails without forwarding.
    - All incoming and outgoing emails on the Exchange Server will be logged for security and auditing purposes.

# Password Security Policy

## General Requirements

* + - All system-level passwords (e.g., root, admin, application accounts) must be changed at least once in a month.
    - All user-level passwords (e.g., email, web, desktop) must be changed every 2 months, with a recommended change interval of 1 month.
    - Passwords must be strong enough.

## Password Management

* + - Employees are encouraged to use a company-approved password manager for secure storage.
    - Passwords must not be shared, written down, or stored in unencrypted files.
    - Multi-Factor Authentication (MFA) is mandatory for accessing critical systems, including code repositories and client databases.

# Data Protection Policy

## Data Handling

* + - Sensitive data, including blockchain smart contracts and client information, must be encrypted during storage and transmission.
    - Employees must not store sensitive data on unsecured devices or share it via unencrypted channels (e.g., personal email).
    - Access to sensitive data is granted on a need-to-know basis, managed through role-based access controls.

## Storage Media Restrictions

* + - Employees are prohibited from moving or using storage media (e.g., floppy disks, CDs, USB drives) without email authorization from the Network Team.
    - Employees must not bring storage media onto the premises without permission.
    - Use of FTP for personal work is strictly prohibited.

## Compliance

* + - Antier Solutions complies with data protection laws, including GDPR and India’s Digital Personal Data Protection Act (DPDPA) 2023, for handling personal and client data.
    - Employees must report any data breaches or unauthorized access to the IT team within 1 hour via [ithelpdesk@antiersolutions.com](mailto:ithelpdesk@antiersolutions.com)

# Network and Server Access Policy

## Server Room Access

* + - Only authorized personnel are allowed entry into the Network Server Room.
    - The Network Team has the authority to inspect any work area or workstation for compliance with this policy.

## Database and Port Access

* + - MS-SQL/MySQL ports (1433/3306) or other database connection ports will be open only for users requiring remote database access, with approval from a higher authority (e.g., Program Manager or Department Representative).
    - Frequent firewall changes may lead to inconsistencies; port open requests must be initiated by the concerned Program Manager or Department Representative.

## Bandwidth Management

* + - Bandwidth allocation will be assigned on a priority and group basis to ensure optimal performance for critical tasks.

# Software Management Policy

## Installation and Uninstallation

* + - Installation or uninstallation of software, including trial versions, requires prior permission from the IT Department.
    - Waivers must be pre-approved by the COO and communicated to the Network Team.
    - Unauthorized installations found during random audits will be the sole liability of the employee, with potential disciplinary action.

## Approved Software

* + - Only IT-approved software may be used for company tasks. A list of authorized tools is maintained in the internal knowledge base.
    - Use of unapproved software (shadow IT) is prohibited due to security risks.

## AI and Large Language Models (LLMs)

* + - Employees must not input sensitive company data into external AI tools like ChatGPT, as this risks data exposure.
    - Internal AI tools developed by Antier Solutions may be used, provided they comply with security standards.

# Company Assets Policy

## Responsibility

* + - Once an asset (e.g., laptop, monitor) is issued to an employee by the IT Department, the employee is fully responsible for its safety and security.
    - Minor wear and tear is acceptable, but employees are liable for serious damage and must cover repair costs or provide a replacement.

## External Storage Devices

* + - No external storage devices (e.g., USB drives, external hard drives) may be attached to company computers without prior approval from the IT Department.

# IT Helpdesk Support

## Request Process

* + - All network support requests must be submitted to the IT Department via email or message.
    - Helpdesk requests will be handled by the Network Team.

## Escalation Process

* + - If a user does not receive a response from the Helpdesk Team, they may escalate the issue by emailing [ithelpdesk@antiersolutions.com,](mailto:ithelpdesk@antiersolutions.com) with the concerned person in CC.

# Employee Training and Awareness

* All employees will undergo mandatory information security training upon onboarding and annually thereafter.
* Training will cover phishing prevention, password management, data protection, email security, and code repository management.
* Ongoing support is available via [ithelpdesk@antiersolutions.com.](mailto:ithelpdesk@antiersolutions.com)

# Policy Enforcement

* The IT Team, in collaboration with HR, will monitor compliance with this policy through regular audits and system logs.
* Violations will result in progressive disciplinary action, starting with a warning and escalating to termination for repeated or severe offenses.
* Unauthorized code publishing or data breaches may lead to legal action if they involve intellectual property theft or illegal activities.
* **Strict Action for Breaches**: Any individual found breaching this policy will face strict action, which may include immediate termination, legal proceedings, and liability for damages caused to the organization, ensuring accountability and safeguarding Antier Solutions’ assets and reputation.

# Review and Updates

* This policy will be reviewed annually or as needed to address emerging threats, technological changes, or business needs.
* Updates will be communicated to all employees via email and the HRMS portal.

# Contact Information

* **Helpdesk**: [ithelpdesk@antiersolutions.com](mailto:ithelpdesk@antiersolutions.com)
* **HR or General Queries**: [hroperations@antiersolutions.com](mailto:hroperations@antiersolutions.com)
* **Registered Office**: C208, Phase VIII-B, Industrial Area, Mohali, Punjab-160059
* **Website**: [www.antiersolutions.com](http://www.antiersolutions.com/)