Information Security Policy
for Internet Platforms

1. Purpose

This Information Security Policy establishes management direction and requirements for the protection of information assets and services provided by the platform, ensuring data confidentiality, integrity, and availability.

2. Scope

This policy applies to all employees, contractors, and third-party users who access, manage, or maintain the platform and its associated information assets.

3. Information Security Principles

- Protect all user and company data from unauthorized access, disclosure, modification, or destruction.
- Comply with all relevant legal and regulatory requirements, including privacy laws.
- Promote a culture of security awareness among all personnel.

4. Access Control

- Grant access to systems and data strictly on a need-to-know basis.
- User accounts must be unique and protected by strong passwords or multi-factor authentication.
- Review and update access rights regularly.

5. Data Protection

- All sensitive information must be encrypted during transmission and storage where applicable.
- Data retention and disposal shall comply with legal and business requirements.

6. System and Network Security

- Keep all software and systems up-to-date with security patches.
- Implement firewalls and intrusion detection/prevention systems.

7. Incident Response

- Report all suspected security incidents immediately to designated personnel.
- Document, investigate, and resolve incidents following established procedures.

8. User Responsibilities

- Do not share passwords or account details.
- Report lost or stolen devices immediately.

- Follow guidelines for accepting, transferring, and storing sensitive data.

9. Policy Review

This policy will be reviewed and updated annually or as required to ensure its effectiveness and compliance with current standards.

10. Enforcement

Violations of this policy may lead to disciplinary action, up to and including termination and legal proceedings.