

GCSTIMES Business Ethics Management Policy

Version 1.1, Effective December 2024

Objective

GCSTIMES is committed to establishing and maintaining a robust business ethics management system to ensure that all business operations adhere to the highest ethical standards, uphold corporate integrity, and promote long-term sustainable development. This Business Ethics Management Policy (hereinafter referred to as the "Policy") aims to regulate the company's business ethics management, ensure compliance with laws and regulations, promote fair competition and integrity, and enhance corporate reputation and social image. We will continuously review this Policy and reserve the right to add or modify requirements at any time.

Scope

This Policy covers all business activities within and outside the company and applies to all employees, management personnel, and business partners who have commercial relationships with GCSTIMES, including but not limited to suppliers, customers, and other relevant stakeholders.

Responsibilities and Authorities

Sustainability Department: Responsible for formulating and implementing the company's business ethics management policy.

Business Ethics Compliance Committee: Composed of leaders from the Supply Chain Center, Administrative Center, and Compliance & Risk Control Center, this committee undergoes regular business ethics compliance training and conducts annual risk assessments and compliance supervision of the company's business ethics management policies.

Employees: Expected to actively participate in and comply with the company's business ethics management policy, report any violations in a timely manner, and cooperate with relevant investigations.

1. Policy

1.1 Anti-Corruption and Anti-Bribery

- Any form of corruption and bribery is strictly prohibited, including but not limited to offering or accepting bribes, improper benefits, or undue advantages.
- Employees must not offer money or other benefits to individuals or institutions to obtain improper advantages, nor may they accept bribes.
- Strict approval procedures and supervisory mechanisms must be established to prevent employees from accepting or offering gifts or hospitality that may influence fair decision-making.
- Business partners will be screened annually, and companies with corruption risks will be excluded. All financial transactions must be truthful, accurate, and transparent.

- A whistleblowing channel must be established to encourage employees to report corruption and bribery incidents, ensuring whistleblower confidentiality and security.

1.2 Information Security Protection

- Customer data, company confidential information, and other critical assets must be protected. Sensitive data must be encrypted during transmission.
- Employees handling confidential information must sign a confidentiality agreement and are strictly prohibited from disclosing sensitive company information.
- Employees may not lend, share, or transmit company information without authorization. The use of unauthorized devices for storing or transmitting company files is strictly prohibited.
- Encryption technology must be employed to protect communications and data transmission. The spread of malware, viruses, or other harmful programs is prohibited.
- An access control mechanism must be established to ensure that unauthorized personnel cannot access confidential information.
- Regular cybersecurity inspections must be conducted, and security measures such as firewalls and intrusion detection systems must be implemented.

- Annual information security training must be conducted to enhance employee awareness and establish an emergency response mechanism.

1.3 Fraud and Money Laundering Prevention

- Employees must uphold the principle of integrity, and any form of fraud or money laundering is strictly prohibited, including false advertising, financial falsification, etc.
- All reports and information must be truthful and accurate. The company prohibits the use of misleading information in product promotions or advertising.
- Tampering with financial statements, accounting records, or using internal information for personal gain is strictly prohibited.
- The company will conduct annual financial audits and collaborate with third parties when necessary to ensure financial clarity and compliance.

1.4 Conflict of Interest Management

- Any form of conflict of interest is prohibited. The company will annually promote professional ethics guidelines to ensure employees adhere to ethical conduct.
- An independent review committee will be established to address conflict of interest issues and ensure fair and transparent resolutions.
- Employees are strictly prohibited from using internal information for personal trading or providing undue benefits to related parties for business advantages.

2. Management Objectives

2.1 Anti-Corruption and Anti-Bribery Objectives

By 2028, 100% of employees will have undergone anti-corruption and anti-bribery training.

By 2028, the company aims for zero occurrences of corruption and bribery incidents.

2.2 Information Security Protection Objectives

By 2028, the confidentiality agreement signing rate and information security training coverage will both reach 100%.

By 2028, the occurrence of information security incidents will be reduced by 5%.

2.3 Fraud and Money Laundering Prevention Objectives

By 2028, the occurrence of fraud and money laundering incidents will be zero.

By 2028, the company's financial records will remain clear and error-free.

2.4 Conflict of Interest Management Objectives

By 2028, the number of conflict of interest incidents within the company will be limited to three or fewer.

By 2028, the reporting and resolution rate of employee conflicts of interest will reach 100%.

3. Responsibilities and Obligations

All departments and employees must strictly adhere to this Policy. The company will continuously improve its internal management system. All management personnel must take the lead in implementing and supervising the Policy and conduct regular evaluations and optimizations.

4. Violation Handling Measures

Employees found in violation of this Policy will be subject to disciplinary actions based on the severity of the offense, including:

- *Severe Violations* (e.g., bribery, fraud): Immediate termination of employment, and in serious cases, reporting to law enforcement authorities.
- *Managerial Negligence*: Demotion, severe warnings, or other disciplinary actions.
- *Financial Losses*: The violator must return any illicit gains and compensate the company for damages.
- *Career Limitations*: Cancellation of performance bonuses and promotion eligibility.

If an action constitutes a criminal offense (e.g., embezzlement, trade secret theft), the company will pursue legal action.

5. Supplementary Provisions

This Policy will take effect on December 21, 2024, with the next update scheduled for May 21, 2025. Any violations or failures to implement this Policy will be subject to corresponding consequences.