SOP Title:

ETHICS

SOP ID / Version Control

Field	Details
SOP Number	SOP/ETH/001
Version	1.0
Date of Creation	01/01/2022
Last Reviewed	31/03/2025
Next Review Date	31/03/2026
Approved By	Pradeep Kumar Dungarwal

1. Training on Corruption and Bribery Prevention

The company will provide training to all employees on the prevention of corruption and bribery. This will cover topics such as recognizing signs of bribery, understanding anti-corruption laws, and company-specific anti-bribery policies.

Objective: Ensure all employees are informed and understand how to prevent and report corruption and bribery.

2. Anti-Corruption Due Diligence on Third Parties

The company will implement a due diligence program on third parties, ensuring that any business relationships align with ethical standards and comply with anti-corruption laws.

Objective: Assess and mitigate risks of corruption from third-party partnerships, suppliers, and contractors.

3. Whistleblower Procedure for Corruption and Bribery

The company will have a clear whistleblower procedure for stakeholders to report any incidents of corruption and bribery. This procedure will ensure confidentiality and protection against retaliation for whistleblowers.

Objective: Create a safe, confidential platform for reporting unethical practices related to corruption and bribery.

4. Corruption Risk Assessments

Corruption risk assessments will be performed regularly to identify and mitigate potential risks within company operations and third-party relationships.

Objective: Continuously identify and manage risks related to corruption and bribery.

5. Audits of Control Procedures to Prevent Corruption and Bribery

The company will conduct regular audits of its internal control procedures to ensure that effective measures are in place to prevent corruption and bribery.

Objective: Ensure the effectiveness of internal controls in preventing corruption and bribery.

---

6. Specific Approval Procedure for Sensitive Transactions

A specific approval procedure will be implemented for sensitive transactions, ensuring that any transaction with a high potential for corruption or bribery is subject to additional scrutiny and approval.

Objective: Provide additional oversight for high-risk financial transactions to prevent corruption and bribery.

---

7. Training on Information Security

The company will provide training on information security to all employees, covering topics such as data protection, cybersecurity threats, and safe handling of confidential information.

Objective: Ensure employees are equipped to handle information securely and prevent breaches.

---

8. Information Security Due Diligence on Third Parties

The company will implement due diligence programs for third-party partners to ensure their practices comply with the company's information security policies.

Objective: Mitigate risks associated with third-party information security vulnerabilities.

---

9. Whistleblower Procedure for Information Security Concerns

A whistleblower procedure will be established for stakeholders to report information security concerns. This procedure will provide protection to those who report breaches or potential security issues.

Objective: Create a secure channel for reporting information security issues while protecting the whistleblower from retaliation.

---

10. Information Security Risk Assessments

Regular risk assessments will be performed to evaluate the effectiveness of information security controls and identify vulnerabilities.

Objective: Identify and mitigate risks related to information security, ensuring the integrity and confidentiality of company data.

---

11. Audits of Control Procedures to Prevent Information Security Breaches

The company will conduct audits to assess the control procedures in place to prevent information security breaches. These audits will help identify weaknesses and recommend corrective actions.

Objective: Ensure that control procedures for information security are robust and effective in preventing breaches.

---

12. Incident Response Plan (IRP) to Manage Breaches of Confidential Information

An Incident Response Plan (IRP) will be developed to manage the breach of confidential information. The IRP will outline clear steps for identifying, reporting, and mitigating security breaches.

Objective: Ensure a swift and coordinated response in case of an information security breach.

---

13. Implementation of a Records Retention Schedule

The company will implement a records retention schedule to manage the storage, access, and disposal of sensitive and confidential information in accordance with legal and regulatory requirements.

Objective: Ensure that confidential information is properly stored and disposed of according to legal requirements.

Acknowledgment

I, Pradeep Kumar Dungarwal, hereby confirm that the policies outlined in this SOP reflect the commitment of Varsha Stones International Private Limited to uphold high ethical standards in all operations. This document serves as a guideline for employees to align their actions with our company's goals for preventing corruption, bribery, and ensuring information security.

For Varsha Stones International Pvt. Ltd.

Signature:
Director

Date: 1st January 2022