



**VATSA CAPITAL VENTURE PRIVATE LIMITED**



## **CHINESE WALL POLICY**

**(As per the requirement of Regulation of SEBI (Merchant Bankers) Regulations, 1992)**

- (i) The document has been prepared in accordance with the Securities and Exchange Board of India (Merchant Bankers) Regulations, 1992, as amended from time to time as per the requirement.
- (ii) The purpose of the Document is to provide essential information about the company in a manner to assist and enable the investors/clients in making an informed decision for engaging the company.
- (iii) The document contains necessary information about the company required by an investors/client before availing services, and the investors/clients may also be advised to retain the document for future reference.
- (iv) This Document is dated 27-02-2026

### **Details of the Company**

Name of Merchant Banker	Vatsa Capital Venture Private Limited
Registered Office Address	4-C/6, 2 <sup>nd</sup> Floor, New Rohtak Road, Karol Bagh, New Delhi-110005
Phone No(s)	01140456969
E-mail address	<a href="mailto:info@vatsacapitalventure.com">info@vatsacapitalventure.com</a>
Website	<a href="https://vatsacapitalventure.com/">https://vatsacapitalventure.com/</a>

### **Details of the Compliance Officer**

Name of Compliance Officer	CS Manish
E-mail Address	<a href="mailto:investors.grievances@vatsacapitalventure.com">investors.grievances@vatsacapitalventure.com</a>



# **CHINESE WALL POLICY**

## **1. OVERVIEW**

The Chinese wall policy, in the context of financial institutions, was introduced in India by the Securities and Exchange Board of India (Insider Trading) (Amendment) Regulations, 2002. These regulations made it mandatory for (i) all listed companies and (ii) other organizations associated with securities markets (financial institutions), to have a Chinese wall policy as a part of their code of internal procedures and conduct. It also recognized implementation of a Chinese wall policy as a valid defense against insider trading allegations. Regulation 12 of the SEBI (Prohibition of Insider Trading) Regulations, 1992 (“Regulations”) requires such organizations to frame an Internal Code in accordance with the ‘model code’ specified in Schedule I of the Regulations (“Model Code”). The Internal Code should be framed ‘without diluting’ the Model Code. Prescribed by SEBI and the organizations should adopt appropriate mechanisms and procedure to enforce such Internal Code. The purpose of this policy is that all the employee/department/division should comply with an information barrier in their day-to-day operations. By virtue of being an organization associated with securities market (broker/ sub- broker, depository participant, clearing/ trading member, merchant banker, custodian etc.) are under an obligation to implement an Internal Code which contains provisions of Chinese wall framework.

## **2. INTRODUCTION**

Customer relationships and information should be treated in the strictest confidence, making every effort to avoid intentional or unintentional disclosures. Any inappropriate disclosure and misuse of any Unpublished Price Sensitive Information or any other confidential customer information (together the “Confidential Information”) could expose The Company and its representatives to severe regulatory and financial obligations/penalties. In addition, any Insider Trading investigations initiated, or violations proven could have, both a severely damaging effect to the business prospects and the reputation of The Company, in the eyes of customers, other regulators/governmental agencies, shareholders, other stakeholders and the media. Information given to The Company by customers, or the information developed based on knowledge and data obtained while dealing with customers is to be adequately protected from improper disclosure or its use in other unrelated business decisions or by unrelated areas. This is required to abide by our confidentiality obligations towards customers, and to avoid the appearance of impropriety, as well as to comply with the Regulations.

## **3. PURPOSE**

This Chinese Walls Policy serves to safeguard and regulate the flow of Confidential Information among the concerned representatives and to prevent unauthorized access to such information. It also provides a control framework to ensure that:



- i. Confidential Information is restricted to the businesses where it belongs.
- ii. Management tools to manage the prevention of conflicts of interest,
- iii. Ensure the segregation of duties or functions and prevention of insider information situations.
- iv. Monitoring procedures to enable us to judge the effectiveness of the controls; and
- v. Safeguarding procedures to be followed if and when such information necessarily has to be distributed internally.

#### 4. **OBJECTIVE**

This policy outlines the procedures and controls (the "Chinese Wall") that are established to restrict the flow of sensitive, confidential, and non-public information between the departments of the company. The purpose is to:

- Prevent conflicts of interest;
- Ensure the segregation of duties or functions and avoid misuse of unpublished price-sensitive information (UPSI);
- Monitoring procedures to enable us to judge the effectiveness of the controls;
- Safeguarding procedures to be followed if and when such information necessarily has to be distributed internally; and
- Ensure regulatory compliance (e.g., SEBI (Prohibition of Insider Trading) Regulations, 2015, and SEBI (Merchant Bankers) Regulations, 1992).

#### 5. **CHINESE WALL FRAMEWORK**

The Company shall maintain information barriers separating Inside Areas from Public Areas to prevent unauthorized communication or misuse of confidential information.

Access to UPSI shall strictly follow the **need-to-know principle** and shall be monitored by the Compliance Officer.

#### 6. **SEGREGATION OF BUSINESS DIVISIONS**

##### i) **Functional Separation**

- Divisions shall function independently.
- Separate reporting lines and departmental heads.
- No overlap in duties or responsibilities.

##### ii) **Physical Separation**

- Access-controlled workspaces shall be maintained where UPSI is handled.
- Confidential documents and meeting rooms shall remain secured.
- Visitor access shall be regulated and recorded.



### iii) Technological Separation

- Separate IT systems, emails, drives, databases, and client management tools.
- Access controls and password-protected systems to limit access to UPSI.

## 7. RESTRICTED ENTRY

The following persons shall **not** enter Inside Areas or access UPSI unless formally authorized:

- employees from Public Areas;
- interns or temporary staff not assigned to the project;
- marketing or sales personnel;
- external visitors without approval;
- any person without legitimate business purpose.

## 8. PENALTY FOR UNAUTHORIZED ENTRY OR ACCESS

Any unauthorized entry into Inside Areas or unauthorized access, attempt to access, or misuse of UPSI shall constitute a **serious breach** of this Policy.

Such contravention may result in:

- immediate withdrawal of access privileges;
- written warning or reprimand;
- suspension from duties;
- monetary penalties or recovery of losses, where applicable;
- termination of employment or contractual engagement;
- reporting to SEBI or other regulatory authorities; and
- initiation of civil or criminal proceedings under applicable laws, including insider trading regulations.

Accidental access must be immediately reported to the Compliance Officer.

Failure to report accidental access shall also be treated as a violation.

## 9. INFORMATION FLOW CONTROL

**i) Restricted List:** Securities in which trading is prohibited due to the Company's involvement in merchant banking assignments.

**ii) Trading Restrictions:** No employee in possession of UPSI may trade in that security.

**iii) Wall-Crossing Protocol:** In special cases, if it is necessary for a person from one department to access information of other department, it must be approved by the Compliance Officer. Further, individuals must sign a Wall Crossing Acknowledgment Form and agree to be classified as "temporary insiders."

## 10. STRUCTURED DIGITAL DATABASE (SDD)

The Company shall maintain a Structured Digital Database as required under Regulation 3(5) of SEBI (PIT) Regulations, 2015 recording:



- persons sharing UPSI;
- persons receiving UPSI;
- PAN/identifier;
- date and time;
- purpose of sharing.

The database shall have audit trails and safeguards against tampering.

## **11. WALL-CROSSING PROCEDURE**

Where access to UPSI is necessary:

- prior approval of Compliance Officer shall be obtained;
- wall-crossing acknowledgment shall be signed;
- individual shall be treated as a temporary insider;
- trading restrictions shall apply.

## **12. DETAILED REQUIREMENTS**

The company requires the employees/directors/departments/divisions to maintain confidentiality of all price's sensitive information. They are prohibited from passing on such information to any person directly or indirectly by way of making a recommendation for the purchase or sale of securities. The price sensitive information should be handled on a "need to know" basis. This means that such information should be disclosed only to those within the company who need the information to discharge their duty.

The files containing confidential information should be kept secure and should have adequate security of login and password etc. The company also requires the organization to adopt this policy which separates "inside areas" from "public areas" for preventing the misuse of confidential information. The "inside areas" are defined as those areas of the organization which routinely have access to confidential information and "public areas" are defined as those areas which deal with sales, marketing, investment advice or other departments providing support services. The Regulations stipulates the following measures to be adopted by organizations for separating "inside areas" from "public areas".

- The employees in the "inside area" should not communicate any price sensitive information to anyone in "public area".
- The employees in "inside area" may be physically segregated from employees in "public area".
- Demarcation of the various departments as "inside areas"
- Only in exceptional circumstances, employees from the public areas may be brought "over the wall" and be given access to confidential information on the basis of "need to know" criteria.
- Employees in the "public area" should not have access to any file or database that contain such Information (including email).



- vi. Employees in the “public area” are prohibited from attending client meetings when Confidential Information is likely to be disclosed or discussed.
- vii. Employees in the “public area” are prohibited from contacting officers or employees of any Company (client) for the purpose of obtaining Confidential Information. The Public Person may, however, call the client’s authorized spokesmen to inquire about facts, events, or transactions as long as the Public Person clarifies his or her role and the purpose of the call.
- viii. Also, the Public Person must state that he or she is not seeking any information that would not be disclosed to the public if inquired.
- ix. When an Employee in the “public area” comes across Confidential Information (either intentionally or unintentionally) that relate to an issuer of publicly traded securities, such Employee should:
  1. Report the matter immediately to the Compliance Officer,
  2. Make no further disclosure of such information,
  3. Stay away from engaging in, recommending, advising or suggesting any transactions that relate to that particular security without obtaining the approval of the Compliance Officer.

### **Obligations**

A Chinese wall is employed between the corporate-advisory area and the brokering department to separate those giving corporate advice on fund-raising, takeovers, etc. from those advising clients about buying securities. The "wall" is thrown up to prevent leaks of corporate inside information, which could influence the advice given to clients making investments and allow staff to take advantage of facts that are not yet known to the public.

### **13. EMPLOYEE CONDUCT**

- Employees must maintain the confidentiality of UPSI.
- No communication of UPSI to friends, family, media, or unauthorized colleagues.
- Avoid discussing confidential information in public spaces.

### **14. COMPLIANCE MECHANISM**

- Compliance Officer shall maintain and monitor restricted list.
- Approve wall-crossing requests.
- Conduct periodic audits and surveillance of trading activity.
- Investigate any suspected breach of the policy.

### **Trading in Company Securities**

The company requires that securities or shares of a listed company should be put on a “restricted/grey list” while the organization is handling any assignment for such listed company



or while preparing appraisal report or while handling credit rating assignments and is privy to price sensitive information.

Additionally, any security which is being purchased or sold or is being considered for purchase or sale by the organization on behalf of its clients/schemes of mutual funds, etc. should also be put on the "restricted / grey list". The effect of putting/ adding a security on the "restricted / grey list" is that any trading in such securities by employees/directors/partners of the organization would require the preclearance of trade by compliance officer. As a result of this, trading in these securities may be blocked or may be disallowed at the time of pre-clearance by the compliance officer after taking into account, all the relevant circumstances.

## **15. CONFIDENTIALITY**

All information obtained from any employee pursuant to this policy shall be kept in strict confidence, except that such information will be made available to any regulatory or self-regulatory organization to the extent required by law, regulation, or this policy.

## **16. POLICY ENFORCEMENT**

### **Failure to Comply with this Policy**

The misuse of confidential information may violate contractual obligations of The Company and its employees, local securities laws, and/or other legal and regulatory requirements.

The Company employees who violate securities laws by purchasing or selling securities based on inside information may subject themselves, as well as The Company, to severe civil and criminal penalties. These penalties may also be applicable to those who "tip" or otherwise assist others in effecting such transactions. In addition, even the appearance of the misuse of confidential information may be extremely damaging to the reputation of the Company and/or their employees. Accordingly, a failure to comply with the policies and procedures set forth in the Company Chinese Wall Policy may be grounds for disciplinary action, including termination of employment for cause. Should questions regarding the Company employee's personal trading activities pursuant to this policy arise, there will be referred to Compliance Officer for review and action, if required.

## **17. MONITORING**

The Company takes seriously its obligation to monitor the activities of its employees and to review the periodically. Compliance Officer will monitor employee day to day activities. All noted deviations from the policy requirements will be referred to the employee for follow-up and resolution (with a copy to be supplied to the employee's supervisor).



## **18. BREACH AND DISCIPLINARY ACTION**

Any breach of this policy will be considered a serious violation.

Disciplinary action may include:

- i. Warning or reprimand
- ii. Suspension or termination
- iii. Regulatory reporting
- iv. Legal action or financial penalties

## **19. THE COMPANY RIGHT FOR ACTIONS**

The Company reserves the right to terminate any employee who breaches this policy. Any such termination may be at the employee's expense and risk.

