SITI NETWORKS LIMITED

(CIN L64200MH2006PLC160733)

Regd. Off: Unit No. 38, 1st Floor, Madhu Industrial Estate, Pandurang Budhkkar Marg, Worli, Mumbai 400 013

MECHANISM FOR INITIATING INQUIRY IN CASE OF ANY LEAK/ SUSPECTED OF UPSI

SITI NETWORKS LIMITED

Approving Authority:	Board of Directors
Original Issue Date:	May 28, 2015
Current Revision Effective Date:	April 1, 2019
Context:	This Policy is formulated pursuant to Regulation 8 (1) read with Schedule A to SEBI (Prohibition of Insider Trading) Regulations, 2015 covering the practices and procedures for Fair Disclosure of Unpublished Price Sensitive Information in relation to Siti Networks Limited.

Mechanism for initiating inquiry in case of any leak/ suspected of UPSI

Scope and purpose

The purpose of this Policy for Mechanism for initiating inquiry in case of any leak/suspected leak of Unpublished Price Sensitive Information (UPSI) is to formulate the written policies and procedures for inquiry in case of leak of UPSI or suspected leak of UPSI and accordingly initiate appropriate inquiries on becoming aware of leak of UPSI and inform the Board of such leaks, inquiries and results of such inquiries.

Applicability

This Policy adopted in line with the principles enumerated in Regulation 9A(5) of the Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015 (SEBI PIT Regulations) and approved by the Board of Directors of the Company ('the Board') shall be applicable on and from April 1, 2019.

Detection of leak/ suspected leak of UPSI

- Pursuant to any information received from any whistle blower;
- Pursuant to receipt of any UPSI from an outside source (e.g. social media);
- Pursuant to sabotage of systems storing details of UPSI or phishing e-mail attack, planted or unauthorized USB drive in the systems storing UPSI.
- Pursuant to theft/ unauthorised destruction of important physical records or portable equipment.

Identification of manner of leak of UPSI

- Due to accidental disclosure of UPSI and promptly brought to the notice of the Compliance Officer by the concerned person;
- Due to willful breach of the regulations by an Insider resulting in communication of UPSI;
- Due to hacking of systems storing UPSI;
- Due to sabotage of particular system storing UPSI.

Escalation of information about leak/ suspected leak of UPSI

- Informing the MD/Whole Time Director/Executive Director/ CEO and Chairman of Audit Committee about the anomalies identified, manner of detection, manner of leak of UPSI, if any, action taken by Compliance Officer to confirm the leakage.
- Submission of findings along with proof in relation to identification of person responsible for the leak;
- Where clear identification is not feasible, engaging external agencies to investigate and submit report in relation to leak of UPSI.

Producing the suspect before the Audit Committee

- Report of investigation to be provided to the Audit Committee;
- The Audit Committee shall provide the right to be heard to the suspect;

- The Audit Committee shall inquire to the suspect about manner in which the breach was carried out, details of any persons assisting in the crime, amount of gain made by the suspect. This will be independent of the findings made in the report presented by the Compliance Officer or external agency, as the case may be.

Action against the guilty

- Once the allegations are fully substantiated, the Audit Committee shall determine the action to be taken against the guilty viz. wage-freeze, suspension from employment, ineligibility for future participation in employee stock option plans, recovery, clawback, etc.
- The Compliance Officer shall inform about the violation of the Regulations and action taken by the Company to SEBI.

Noting by the Board

- Details of violation and the action taken against the guilty shall be informed the Board of Directors.

Sensitizing the Employees

- Appropriate sharing of event information with the correct components, while maintaining confidentiality and protecting privacy in order to ensure the consequences are clearly communicated to all employees and acts as a deterrent.

Plugging the gaps

- Basis the findings of the investigation, existing processes, controls and procedure to be revisited and strengthened to avoid similar incident in future.