# SOFTVAN LTD.

## CYBER SECURITY POLICY

**Objective:**

Adopting a robust IT Framework in which the IT environment functions such that the IT objectives support the business to meet the Overall business objectives. IT Activities undertaken have to observe compliance with the provisions of the Information Technology Act & other Regulatory Acts, as applicable to the entity Information security is established by imbibing principles of confidentiality and integrity around the information received, stored, and transferred within & outside the organisation. Softvan Limited considers these factors in aiming the IT forefront, now limited to the internal processes, as support to its various business activities.

**Scope and Applicability:**

Outlining the list of policies addressing the Information technology and Security aspects. These shall be followed at an entity level, as applicable, by all the employees spread across all the locations of the Softvan Limited.

**Cyber Security Policy Statement:**

**Softvan Limited shall be in its consistent and truthful efforts to:**

- Manage the data by bringing up suitable policies to gather, store, process and disposed of, with needful measures through its life cycle ensuring security, accuracy, availability and usability.
- Identify and track the most valuable Information Assets and managing various risks involved to make it available for continuous business process.
- Maintain cyber security discipline by managing user identify and access permission on its computer networks.
- Create systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions.
- Guide the users for their consistent and secured management of passwords of individual privileges allowed on various application platforms, which will prevent unauthorised access of sensitive information.
- Formalise a structured approach to ensure the changes to system are introduced and controlled and coordinated to conduct a better change management cycle

- Define, conduct and periodically review the Software Development Lifecycle (SDLC) & adapting refined process and procedures in standard norms of compliances.

- Identify and analyse the events and incidents for their nature conduct adequate corrective measures to avoid its occurrences in future.

- Implement various methods and process to protect the electronic data and strengthen the ability to withstand or recover from cyber events which disturbs normal business operations with the help of better cyber resilience strategy and IT ecosystem.

- Maintain proper observations to ensure and manage business continuity and disaster recover at the relevant areas, where the dependence of Information System process and practices are in practice.

- Develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

**Review & Reporting:**

- The Policy is to be reviewed periodically and deviations to be reported on an immediate basis for a corrective action.

The Policy was approved by the Board of Directors of the Company vide Board Resolution dated 30th March, 2025 and will be effective from the date of listing of stock exchange.

CHAIRMAN AND MANAGING DIRECTOR /

EXECUTIVE DIRECTOR