ASTRAL

# INFORMATION SECURITY POLICY

At Astral, we embrace a security-first culture, ensuring that our people, processes, and technologies work together to protect the information assets entrusted to us. Our goal is to enable fearless innovation and growth by building a secure and resilient digital ecosystem. We are committed to enhancing stakeholder trust by:

### 1. Complying with Laws and Regulations

We adhere to all applicable information security, privacy, and data protection laws, ensuring legal and ethical handling of information.

### 2. Embedding Security into Business Processes

We integrate information security principles into every function—ensuring confidentiality, integrity, and availability of data throughout its lifecycle. Security is considered at every stage of business planning, operations, and transformation.

### 3. Building Awareness and Accountability

We nurture a culture of security through continuous education, awareness programs, and clear accountability. Every employee and partner understand their role in protecting information assets.

### 4. Strengthening the Information Security Management System (ISMS)

We maintain a robust ISMS, aligned with Industry Standards, that is regularly reviewed, audited, and improved to meet evolving business needs and emerging threats.

### 5. Adopting Advanced Security Technologies

We leverage modern tools and practices, including access controls, encryption, network monitoring, and threat intelligence, to proactively manage and mitigate risks in the evolving cyber threat landscape.

### 6. Protecting Personal and Sensitive Data

We handle personal and sensitive information responsibly and ethically, and ensure data privacy through secure collection, processing, storage, and disposal practices.

### 7. Managing Third-Party Risks

We ensure that all vendors, contractors, and partners adhere to equivalent security standards. Third-party engagements are governed by clear security requirements and regular assessments.

### 8. Ensuring Incident Readiness and Response

We are prepared to detect, report, and respond to security incidents promptly, minimizing impact and learning from each incident to strengthen our defenses.

## 9. Establishing Responsibilities for Information Security

Everyone at Astral plays a role in keeping information secure—employees, contractors, and third-party users. Each individual is responsible for:

- Following information security policies and procedures.
- Protecting the data and systems entrusted to them.
- Reporting any suspected or actual security incidents without delay.
- Participating in security awareness and training programs.
- Cooperating during audits, assessments, or investigations.

## Our Commitment

Astral is dedicated to building and maintaining a secure, resilient, and trusted digital environment. By continuously improving our practices and technologies, we ensure that our stakeholders can innovate, grow, and operate with confidence.

**(Hiranand Savlani)**
**Whole Time Director & CFO**

**30 Sep 2024**