# ARISTA SYSTEMS PVT. LTD., NAGPUR

## Information Security Compliance

Arista Systems Pvt. Ltd., Nagpur maintains an Information Security Program to ensure the confidentiality, integrity, and availability of all computer and data communication systems while meeting the necessary legislative, industry, and contractual requirements.

Arista Systems Pvt. Ltd., Nagpur policies, procedures, and standards are based on the International Organization for Standardization (ISO)/International Electro technical Commission (IEC) 27001. In addition, we use an independent third-party body to audit our compliance with leading industry standards periodically.

## ISMS HIGH LEVEL POLICY

- All information assets are used in a manner that supports the strategic goals and objectives of Arista Systems Pvt. Ltd., Nagpur.
- All applicable legal and/or regulatory requirements pertaining to information security are documented and implemented.
- All information & information processing systems are identified, valued and classified to ensure adequate protection.
- An Information Security Risk Management Methodology to assess information security risks is developed and maintained.
- We provide appropriate information security training and awareness to all employees (permanent & contract employees).
- All our employees, vendors or third-party contractors adhere to the information security policies, procedures, standards, guidelines etc. approved by the management of Arista Systems Pvt. Ltd., Nagpur.
- Information is handled in a secure manner to avoid any loss of confidentiality, integrity, and availability during creation, storage, processing, transmission and disposal.
- Information and information processing systems are accessible to the authorized users as per their business needs.
- Information and information processing systems are physically secured from any loss of confidentiality, integrity & availability.
- All changes related to information and information processing systems are managed in a secured manner.
- All information security incidents are reported and managed in a timely manner with proper escalation matrix defined for treating high severity incidents.
- IT Disaster Recovery plans are defined, implemented and tested adequately to ensure availability of information and information processing systems during any crisis/emergency.

- Information security controls are continuously reviewed and improved to ensure continuous adherence to this policy.
- Compliance to applicable standards and regulations on information security e.g. ISO 27001 is ensured.
- Information Security shall be continually improved through implementation of preventive actions.

**Date :** 12/05/2022
Nagpur

**Chief Operating Officer**