ISMS POLICY STATEMENT

The Management of GS1 India recognizes the importance of developing and implementing an Information Security Management System (ISMS) and considers security of information and related assets as fundamental for the successful business operation. Therefore, GS1 India is committed towards securing the Confidentiality, Integrity and availability of information for the day-to-day business and operations..

GS1 India is committed to ensure that the information is only accessible to authorised persons from within or outside the company. An Information Security Management System (ISMS) comprising of the Information Security Policies, Procedures and Processes has been adopted to effectively protect data/information of the organization and its subscribers from information security threats, whether internal or external, deliberate or accidental.

The Management of GS1 India has approved the Information Security Management System Manual and associated policies. The management's commitment is:

- All regulatory and legislative requirements related to GS1 India are met
- The confidentiality of information is protected and prevent disclosure of valuable or sensitive information
- The integrity of information is maintained to ensure its accuracy and completeness
- The availability of information is maintained to meet business needs, subscriber and regulatory requirements.
- Business continuity plans are developed, maintained and tested
- Information security awareness is shared with all employees
- Incident management process is established and implemented to ensure that all breaches of information security, actual or suspected are reported and investigated
- Risks are mitigated to an acceptable level through a risk management framework
- The information security management system is continually improved
- Appropriate resources are allocated in order to implement, operate and review an effective Information Security Management System
- All stakeholders are responsible for implementation of respective security policies and procedures within their area of operation, and oversee adherence by their team members

By implementing ISMS, the management will assure all interested parties that an appropriate and effective information security management system is in place.

The Management shall follow a formal disciplinary process against employees who violates the information security policies and procedures.

The Management will conduct a review of the ISMS at periodical intervals or when significant changes takes place to continually improve and ensure that the system meets the requirements of all stakeholders and compliance to the ISO 27001 standard.

The Management has overall responsibility for maintaining this Policy and providing guidance on its implementation. All managers and team leaders are directly responsible for ensuring that ISMS policies and procedures are followed within their business areas.