# Information Security Policy

## Confidentiality Statement

The policies, procedures and standard practices described in this manual are for the said process only at SG Analytics **(from here on termed as 'SGA')** and do not extend or imply to any other SGA entity. Information in this document represents guidelines only. SGA reserves the right to modify this document, amend or terminate any policies, procedures, or employee benefit programmes whether or not described in this document at any time, or to require and/or increase contributions toward these programs.

All policies contained herein have been adopted by SGA and supersede previous policies. We periodically review policies, in part or as a whole, to ensure that they continue to reflect current thinking of the organisation and are consistent with trends and legal requirements.

# Document Summary

| | |
|---|---|
| **Document Reference #** | SGA_PO_Information Security Policy_v2.1 |
| **Author** | Smitha Saju |
| **Reviewed By** | Rohit Kalghatgi |
| **Approved By** | Rohit Kalghatgi |
| **Owner** | Rohit Kalghatgi |
| **Document Type** | Policy |
| **Document Status** | Approved |
| **Document Circulation** | Confidential Internal |
| **Document View Level** | Internal |
| **Release Date** (dd-mm-yyyy) | 07-03-2017 |

## Revision History

| Version | Date<br>(DD-MM-YYYY) | Author<br>(Designation: Name) | Changes<br>(Short Description) | Remarks |
|---|---|---|---|---|
| v1.0 | 26-07-2016 | Dy. MR<br>Smitha Saju | - | Initial document |
| v1.1 | 02-01-2017 | Dy. MR<br>Smitha Saju | Addition in asset (section 1) and updated the reference section | - |
| v2.0 | 12-01-2017 | Dy. MR<br>Smitha Saju | BUH / DH changed to BU Lead | Reviewed Document |
| v2.1 | 07-03-2017 | Dy. MR<br>Smitha Saju | Change in the address | - |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Content

# 1. Introduction

## 1.1 Objective

Information security policies are essential prerequisite to a sound IT security. This policy is designed to preserve the confidentiality, integrity, availability of SGA's information assets as well as to ensure the continued delivery of services. It is also aimed to establish appropriate focus and standards for acceptable security practices across the organization while complying with regulatory mandates and contractual obligations with clients.

## 1.2 Scope

*"Information Security Management System (ISMS) at SG Analytics Pvt. Ltd. applies to its operations in providing research and analytical services in Investment Research, Data Analytics, Market Research and Business Consulting units along with support functions viz, Information Technology, Human Resource, Administration and Finance."*

### 1 Location

This policy applies to all the employees of SGA, Pune situated at:

SG Analytics Pvt. Ltd., 601, 6th Floor,
Wing "2", Cluster C, EON Free Zone,
Kharadi, Pune, Maharashtra, India - 411 014

### 2 Logical Boundary

The ISMS would govern the networks and technologies of delivery teams, IT, HR, Admin and Finance.

### 3 Assets

This Information Security Policy would be applicable to all its assets including:

a) Information assets (digital) such as emails, processes etc

b) Paper documents such as contracts & SLA's

c) Entire network and hardware assets such core routers, switches, systems, firewalls, etc

d) Computing devices such as Laptops / Desktops, PDA / Tablets / Notebooks / Mobile / Smart phones, Pocket Computer, iPods and Fax machine

e) Storage media assets such as USB / Zip / Pen / Flash Drive , Memory Cards, CD writers / DVD / Blue Ray Disks, Tape Drives , Cartridges, Hard drive, Web cam and Digital Camera

f) Software assets such as WinXP OS, Ms Office etc.

g) Service assets such as HVAC, access control system

h) People (employees)

i) Company's reputation (brand value)

## 1.3 Glossary of Terms

| Terms | Description |
|---|---|
| Admin | Administration |
| BU | Business Unit |
| COO | Chief Operating Officer |
| Dy. MR | Deputy Management Representative |

| | |
|---|---|
| ERR | Enterprise Risk and Resilience |
| HR | Human Resource |
| HVAC | Heating, Ventilating, and Air Conditioning |
| IPR | Intellectual Property Rights |
| ISMS | Information Security Management System |
| IT | Information Technology |
| MR | Management Representative |
| PM | Project Manager |
| SGA | SG Analytics Pvt. Ltd. |

## 2. Responsibility

1. Information security is the responsibility of everyone in SGA
2. MR shall have the responsibility to establish, review , implement , maintain and continually improve ISMS
3. MR and Dy. MR shall be responsible for successful implementation of ISMS in the organization
4. ERR team shall review and update the security policies, processes and procedures
5. ISMS representatives shall implement and maintain the controls.
6. All BU Lead / PM will be directly responsible for ensuring compliance of the policies in their departments / teams

## 3. Guidelines

### 3.1 Policy

1. COO shall give a clear direction and management support for information security initiatives within SGA
2. MR shall be responsible for information security within SGA
3. Dy. MR shall be responsible for coordinating the implementation of information security within the organization and its management. ISMS representatives will comprise of representatives from different business units / departments
4. DY. MR and ISMS representative shall be responsible for coordination of ISMS related activities throughout the organization
5. MR shall release / change information security policy
6. MR shall, based on the organization’s needs and the type of incidents, seek specialist security advice from internal or external consultants
7. MR shall implement ISMS in the organization with the help of various position(s) having their individual / collective role and responsibility in the ISMS framework as defined in ISMS Manual

### 3.2 Vision

*"To enable positive change by collaborating with our customers, fellow SGA'ites and the society."*

### 3.3 Mission

*"Constancy of Purpose - We align all our individual efforts to deliver quality service."*

### 3.4 Values

*Accountability* -We acknowledge and proactively take responsibility for actions and hold ourselves accountable to our clients, colleagues and society for the outcome.

*Reliability* - Punctuality, Certainty and Trustworthiness.

*Meritocracy* - We believe in rewarding our people based on their performance and merits.

*Excellence* - We strive to get the best solution through efforts and innovation.

*Drive* - Passion fuels motivation, motivation drives performance and performance is celebrated with lots of fun and gusto.

### 3.5 Information Security Policy Statement

*SG Analytics Pvt. Ltd. is committed to maintain and continuously improve Information Security Management System (ISMS) that effectively safeguards the interests of its customers, partners and stakeholders.*

*It shall pay attention to the following:*

1) *Maintain confidentiality, integrity and availability of information in all operations, and*
2) *Ensure compliance with best practices, and applicable statutory, regulatory as well as contractual requirements, and*
3) *Ensure secure information processing environment for customers, partners and stakeholders*

### 3.6 Information Security Requirements

1. Business Requirement - IT is an integral part of SGA's business processes. Information in any form is thus most valuable asset for SGA. The list and type of assets is mentioned in Scope of ISMS.
2. Contractual Obligations - The Non Disclosure Agreements signed with customers includes the details about IPR, copyright of the material shared by customer to SGA and delivered to customer by SGA.
3. Legal and Regulatory requirements - MR has identified and maintained a list of laws to comply with, in the compliance register.

### 3.7 Security Objectives

The information security objectives are the basis for design, implementation and monitoring of ISMS. Security objectives for each department in scope shall be published in "*ISMS Objectives Plan – Organisation level*."

### 3.8 Communication of Policy

The policies and procedures shall be published in a shared folder on SGA's intranet portal and communicated to employees and relevant external parties.

### 3.9 Violation of Information Security Policy

Non-compliance or violation of the SGA's information security policy shall result in disciplinary action as per "*Disciplinary Action Policy*" and other such rules prevalent at the time of violation.

### 3.10 Periodic Review

The information security policy shall be reviewed on half yearly basis or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

ERR team would review the policies, the compliance and implementation status, effectiveness of controls and their implementation, taking into account internal audit reports, incidents, suggestions and feedback from related parties and make appropriate recommendation for improvements to MR.

### 3.11 Detailed Policies

This information security policy shall be implemented through specific policies and procedures specified in the "*Master list of document*".

### 3.12 Structure of ISMS

The structure of ISMS along with the roles and responsibilities are defined in "*ISMS Manual*."

## 4. Reference

1. Disciplinary Action Policy
2. Master list of document