Information Security Incident Management

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 Incident Management_v2.0
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	02-01-2017

Revision History

Version	Date (DD-MM-YYYY)	Author (Designation: Name)	Changes (Short Description)	Remarks
v1.0	22-07-2016	Dy. MR Smitha Saju	-	Initial document
v2.0	02-01-2017	Dy. MR Smitha Saju	Change of compliance member	Reviewed & approved document

Content

1. Introduction

1.1 Objective

This policy helps the employees to report, diagnose, resolve and mitigate the effects of security incidents at SGA. It is the responsibility of every employee to protect the business sensitive information that they manage or access. All information security incidents must be reported to minimise any potential risk and impact that may occur as a result of it.

1.2 Scope

This policy applies to all security incidents affecting information and IT assets of SGA.

1.3 Glossary of Terms

Terms	Description
Admin	Administration
Dy. MR	Deputy Management Representative
HR	Human Resource
IT	Information Technology
MR	Management Representative

1.4 Definition

1. Information Security Event: An Information Security event is an identified occurrence of a system, service or network state indicating a possible breach of information security or failure of safeguards, or a previously unknown situation that may be security relevant.
2. Information Security Incident: An Information Security incident is indicated by a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
3. IT Security Incident: IT security incident is defined as an event, which has a notable negative impact on the Organization's information security.

   An IT security incident falls under any of the following types:

   a. Unauthorized access into Organization's IT Systems (such as intrusion, virus attack, etc.)

   b. Exploitation of security weaknesses / vulnerabilities

   c. Software and hardware malfunctions

   d. Misuse of information systems resources

   e. Violation of Organization's policies and procedures

   f. Violation of applicable legal laws and other regulatory conditions

   g. Human Errors

   h. Uncontrolled system changes

   i. Service, facility or equipment loss

4. Non-IT Security Incident: Non-IT security incident is defined as any event, which has a notable negative impact on the Organization's information security and information/IT assets and is non-technical in nature such as:
   a. Lapse in physical security
   b. Thefts
   c. Fire
   d. Environmental hazards

2. Responsibility

MR would be responsible for verifying the effectiveness of the process and its revision whenever required.

	Responsible	Accountable	Consulted	Informed
Recording and Classifying Security Incident	User / Dy.MR	Dy. MR / MR	HR Head	COO
Resolving Non-IT Security Incident	Admin & Dy. MR / MR	Dy. MR / MR	HR Head	COO
Resolving IT Security Incident	IT & Dy. MR / MR	Dy. MR / MR	HR Head	COO
Closure Of the incident and Maintaining Knowledgebase	Dy. MR / MR	Dy. MR / MR	HR Head	COO

3. Policy

3.1 Recording of the Security Incident Activity

1. The employees will update actual / potential occurrence of security incident via email on compliance@sganalytics.com, IT helpdesk or hotline for compliance
2. Each security incident will be identified as "IT security incident" or "Non-IT security incident" as guideline given above
3. This email is received by the compliance members of SGA (Refer Annexure 1 for members)
4. The employee shall not report to or discuss Information Security Incidents with other un-authorized users or persons external to the organization
5. Any attempt to interfere with, prevent, obstruct or dissuade employees in their efforts to report actual / suspected information, whether on account of accidental or intentional acts or violations committed by self or others to those rightfully investigating is strictly prohibited and would be liable for disciplinary action
6. IT shall have access to all critical servers to monitor system use, ensuring that only authorized actions and processes are performed
7. IT shall maintain accurate computer system clock to ensure the accuracy of audit logs, which may be needed for investigation or as evidence in legal or disciplinary cases. Where a computer or communications device uses a real-time clock, it shall be set to

local standard time. Clock timings shall be regularly checked and synchronized with standard local time

8. A formal disciplinary process shall be in place for handling violations of security policies and procedures
9. All Information Security Incidents shall be resolved to ensure that:

   i. The occurrence of such incidents are minimized or eliminated and

   ii. Effective security controls are strengthened and re-established
10. Wherever possible, evidences shall be collected to initiate and support such disciplinary action and later if required prosecution process for violating legal requirements including the Organization's policies and procedures, and emphasis shall be given to ensure that these evidences are fully admissible in the court of law

4. Annexure - 1

Compliance Members	Department
Ankit Maheshwari	Finance
Rohit Kalghatgi	MR - ISMS
Sandeep Datta	Human Resource & Administration
Umed Patil	Information Technology
Smitha Saju	Dy. MR – ISMS