Communication 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_PnP_Communication Policy_v2.0
Author	Smitha Saju
Reviewed By	Rohit Kalghatgi
Approved By	Rohit Kalghatgi
Owner	Rohit Kalghatgi
Document Type	Policy and Procedure
Document Status	Approved
Document Circulation	Confidential Internal
Document View Level	Internal
Release Date (dd-mm-yyyy)	12-01-2017

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	12-01-2017	Dy.MR Smitha Saju	BUH / DH changed to BU Lead	Reviewed Document

Content

1. Introduction

1.1 Objective

The purpose of this procedure is to provide guidelines and instructions for communicating the effectiveness of ISMS, including Information security requirements, objectives, policies and achievements as well as product and process performance information.

The objectives of this procedure are:

1. Adhere to strategic directions for information management
2. Respond to needs and expectations of connecting with internal users
3. Enhance understanding of information used to make decisions
4. Promote efficient and effective sharing while leveraging experience and knowledge of data already collected within SGA
5. Exchange personal information between a public body and a person, a group of persons or an organization, as allowed within company privacy policy

1.2 Scope

This procedure is applicable to exchange the information at all locations of SGA.

Communications received from employees and all components of the public, including customers, media, environmental groups, local agencies and internal communications generated to external parties concerning SGA's Information Security management requirements of ISO 27001:2013 standards.

This procedure applies to the internal and external communication of information relating to:

1. Information security policy & objectives,
2. Procedures,
3. Performance suggestions and feedback both internal and external
4. Importance of meeting service user, statutory and regulatory requirements
5. Changes in service requirements
6. How staff contributes to achieving the Information Security objectives
7. Addressing interested parties requirements and issues

1.3 Glossary of Terms

Terms	Description
BU	Business Unit
COO	Chief Operating Officer
Dy.MR	Deputy Management Representative
ISMS	Information Security Management System
MR	Management Representative
SGA	SG Analytics Pvt. Ltd.

2. Responsibility

The primary responsibility of implementing this policy lies with MR.

	Responsible	Accountable	Consulted	Informed
Basic Information exchange	Information holder	BU Lead	-	-
Critical Information	Information holder / BU Lead	BU Lead	BU Lead	COO

3. Policy

Exchanges of information between organizations should be based on a formal exchange.

The procedures and controls to be followed when using electronic communication facilities for information exchange and prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities should consider the following items:

1. To protect exchanged information from interception, copying, modification, mis-routing, and destruction
2. The detection of and protection against malicious code that may be transmitted through the use of electronic communications should be ensured
3. It shall be ensured that communicated sensitive electronic information is in the form of an attachment are protected
4. Guidelines outlining acceptable use of electronic communication facilities shall be distributed
5. It shall be ensured that use of wireless communications, taking into account the particular risks involved
6. Employee, contractor and any other user's responsibilities not to compromise the organization, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.
7. Retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations
8. Not leaving sensitive or critical information on printing facilities, e.g. copiers, printers, and facsimile machines, as these may be accessed by unauthorized personnel shall be observed
9. Controls and restrictions associated with the forwarding of communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses
10. Reminding personnel that they should take appropriate precautions, e.g. not to reveal sensitive information to avoid being overheard or intercepted when making a phone call by:
    a. people in their immediate vicinity particularly when using mobile phones;
    b. wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers;
    c. people at the recipient's end;

11. Not leaving messages containing sensitive information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling shall be observed

12. It shall be seen that employees are made aware about the problems of using facsimile machines, namely:

    a. sending documents and messages to the wrong number either by misdialling or using the wrong stored number;

4. Procedure

4.1 Internal Communication

Where information for dissemination becomes available to the Project Manager, it is communicated to employees in the next available team briefing or meeting.

Internal communication occurs on an ongoing basis and is achieved through various mechanisms that include, but are not limited to:

1. Team meetings and briefings
2. Training sessions
3. Display boards
4. Computer network / intranet / e-mail
5. Corrective actions
6. Internal memorandums / letters
7. Minutes of meetings
8. The corporate policies and objectives are documented in the integrated system manual
9. The corporate policies are internally communicated via internal portal and training sessions
10. Integrated system procedures are controlled documents
11. Current versions of procedures are communicated to personnel via the controlled document distribution list
12. The integrated system procedures are communicated through internal training sessions

MR has the overall responsibility for ensuring that information and data about performance and the effectiveness of the management system is reported to management.

This includes the distribution of all applicable documents, reports and records to appropriate functions:

1. Performance of information security management system is reported via metrics and audit reports
2. Audit reports are presented at management review meetings

4.2 External Communication

All formal ISMS communications are authorized prior to release. Appropriate advice is sought on the content and dissemination of all formal external communications. Consideration is given to the attributes of the communication media. The use of paper for internal and external communications is minimized in favour of the use of electronic media and the worldwide web.

All external communications regarding SGA's significant ISMS aspects, policies, objectives and targets are forwarded to the Management Forum.

External communications are categorized as the following from external stakeholders:

1. Emails
2. Telephone calls
3. Letters
4. Written requests for information
5. Questionnaires on information security performance
6. Requests for responses to government documents / policies
7. SLA/Contracts

In each case the following information is recorded and stored as a record:

1. Date of communication
2. Name of the person
3. Address (if relevant)
4. Contact details e.g. telephone number and email
5. Type of enquiry e.g. complaint
6. How the communication was received e.g. letter, email or phone call
7. And brief details of the response

The responses to external communications are recorded if they are transmitted by email or letter. In each case the response is stored as a record. All external communication records are stored in accordance with the document and record control procedures.

4.3 Customer Communication

SGA determines and implements effective arrangements for communicating with customers in relation to Information Security events, enquiries, contracts or order handling, including amendments, and customer feedback, including customer complaints for information security. This process ensures adequate understanding of the needs and expectations of interested parties, and for translation into organizational requirements. This process includes the identification and review of relevant information to actively involve customers and other interested parties. Examples of relevant process information include but are not limited to:

1. Requirements of the customer or other interested parties
2. Research, including sector and end - user data
3. Contract requirements
4. Business continuity requirements

4.4 Verifying Effectiveness

The effectiveness of communication is evaluated on an on-going basis; through management reviews, employee surveys, audits and informal discussions.

The effectiveness of the communication process is determined by:

1. Interviewing employees to determine awareness of policies, objectives and management system performance
2. Evaluating non-conformities to determine whether they are linked to poor internal communication
3. Evaluating the relevance and dates of displayed information
4. Examining the feedback mechanisms within the organization
5. Evaluating training and induction programmers within the organization
6. Viewing minutes of meetings containing items of internal communication requirements of the customer or other interested parties

4.5 Suggestions & Feedback

Employees at all levels are encouraged to report problems related to the management system and to offer suggestions on how to improve performance. Employees may communicate these problems or suggestions to their supervisor / Managers through suggestion forms or corrective / preventative action request.

4.6 Review

The effectiveness of our communication process is assessed during review meetings. New communication strategies and processes are implemented where appropriate.

5. Reference

None