Control of Documented Information

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_Control of Documented Information_v3.0
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	26-07-2016	Dy. MR Smitha Saju	-	Initial document
v2.0	19-08-2016	Dy. MR Smitha Saju	Changes made in 5.3 and 5.4	Reviewed and approved version
v3.0	12-01-2017	Dy. MR Smitha Saju	BUH / DH changed to BU Lead	Reviewed Document

Content

1. Introduction

1.1 Objective

To establish and maintain a system for preparation, distribution control and updating of documented information related to Information Security Management System ISO 27001: 2013.

1.2 Scope

The scope for this policy covers documented information pertaining to ISMS at SGA.

The documented information is manifested in documents such as:

1. Manuals
2. Handbooks
3. Policy Documents
4. Procedure Documents
5. Risk Management Documents
6. Audit Documents
7. Risk Analysis and Treatment Documents
8. Record (special type of documents)
9. Control effectiveness dashboards
10. Log Books, results achieved
11. Audit record
12. Minutes of Meeting

Operational documents of departments are **not** covered by this policy even if they may be used as evidence of ISMS, ISMS practices.

1.3 Glossary of Terms

Terms	Description
ISMS	Information Security Management System
BU	Business Unit
Dy. MR	Deputy Management Representative
MR	Management Representative
SGA	SG Analytics Pvt. Ltd.
SOP	Standard Operating Procedure

1.4 Definition

Documented Information - Information required be controlling and maintaining by an organisation and the medium on which it is contained

2. Responsibility

Owners and readers of the documented information are responsible for adhering to this policy and procedure.

3. Policy

1. The employee responsible for drafting and approving controlled documents must ensure conformance to the format and content as outlined in this policy
2. The document owner is responsible for managing the issue, revision, approval , distribution and archiving of the document
3. The Owner mentioned in the policy shall be responsible to keep a tab on timely production, revision and approval of the controlled document applicable to their department
4. BU Lead shall ensure the employees of their unit are trained and comply with the requirement of all SOP's applicable to their department
5. Any change in the policy or procedure should be communicated with document owner
6. All the controlled documents such as policies and procedure, SOPs, manuals need to be reviewed once in every six (6) months
7. All the controlled documents should be appropriately classified for circulation
8. All organisation-wide policies and procedure including ISMS will be uploaded on SGA portal http://sgaeasy/application/#/login

4. Classification of Document

All controlled document shall be classified as Confidential Internal, Confidential Sensitive, Confidential Limited and Public.

1. Confidential Internal – The documents that contains sensitive information about a process, customer, supplier or employee which can be circulated and accessed only within the organization. Example: Policies, Organizational wide SOPs.
2. Confidential Sensitive – The documents that contains sensitive information about a process, customer, supplier or employee which can be circulated and accessed only with a certain group within the organization. Example: Departmental SOPs, Departmental Reports.
3. Confidential Limited – The documents that contains sensitive information about a process, customer, supplier or employee which can be circulated and accessed only with certain group within the organization and limited to few clients / vendors outside the organization. Example: RFPs, Contracts, SOWs, MBRs, QBRs, Reports, Data deliverables
4. Public – The documents which will be available to people outside the organization on a public domain will be termed as Public. Example: Press release, website information

5. Procedure

5.1 Creating and Updating

1. All documents should comprise of a TITLE PAGE. Use the "Calibri" font for all document
2. The second page should comprise the Document Summary which includes the below mentioned list

Document Summary

Document Reference #	
Author	
Reviewed By	
Approved By	
Owner	
Document Type	
Document Status	
Document Circulation	
Document View Level	
Release Date	

Document Reference # - Document reference number should be updated as company abbreviation_document type abbreviation_document name_current version

Company abbreviation is SGA

Document type can be used as per the abbreviation mentioned below.

Document Type	Acronym / Abbreviation
Business Requirement Specification	BRS
Manual	MN
Policy and Procedure	PnP
Policy	PO
Procedure	PR
Record	RCD
Standard Operating Procedure	SOP

Example for Document Reference #: SGA_PnP_Control of Documented Information_v1.0

Author: The first and last name of the employee who prepares the document should be mentioned in this section

Reviewed by: The first and last name of the employee who prepares the document should be mentioned in this section.

Approved by: Mention the first and last name of the employee who approves the document in this section. The document circulated or used at organisation level should be approved by CEO or COO and the document circulated at department level can be approved by BU Lead.

Owner: The first and last name of the employee who is responsible for approval, revision, version control and archival of the document.

Document Type: The documents can be classified as Standard Operating Procedure, Policy, Procedure, Policy and Procedure, Record or Manual.

Document Status: The status of the document is classified as Draft / Reviewed / Approved

Document Circulation: Document Classification needs to be mentioned in this section.

Document View Level: This section defines the department or business unit which has authority to view the document. If mentioned as internal then all employees of SGA can view the document.

3. The third page should encompass the Revision History stated as below

Revision History

Version	Date (DD-MM-YYYY)	Author (Designation: Name)	Changes (Short Description)	Remarks

Version: Version numbering consists of a number followed by one decimal number. The number to the left of the decimal point describes the number of reviews from issue. The numbers to the right of the decimal point describe the number of minor amendments from the time of issue or from the last review.

The first version is always 1.0 and after the first minor amendment, will result in 1.1. Therefore the 9th minor amendment without any review would appear as 1.9; this would not normally occur but is acceptable. Each review would result in the number to the left of the decimal point incrementing by 1 and the number to the right of the decimal point reverting to zero.

The real benefit of this system of numbering is that it provides documented information at a glance. If the version is 1.00 then there have been no changes since issue. However, if for example the version number was 7.06 this would reflect six reviews since the first version was created and six minor amendments since the last review. In other words this particular document has been kept current and been reviewed regularly.

Date: The date on which the version number is changed. It should be updated in dd-mm-yyyy format.

Author: The first and last name & the designation of the employee who drafts the document is mentioned in this section

Changes: It is short description of the changes made in the document.

Remarks: An additional remark that needs to be updated while revising the version.

4. The fourth page shall include the Table of Content named as Content

5.2 Format

1. The Author should structure the document appropriate to its nature. All policies and procedures shall have following sections by default
    a. Objective
    b. Scope
    c. Glossary of Terms
    d. Responsibility
    e. Policy
    f. Procedure
    g. Reference (If required)
    h. Annexure (If required)

5.3 Review and approval for suitability and adequacy

1. Approve documents for adequacy prior to issue
    a. The Dy. MR shall create necessary documents as required for ISMS. BU Lead shall create necessary documents as required for their departments
    b. The newly created document shall be mailed to COO

c. COO / MR shall approve / disapprove the document based on an adequacy review

d. Approved documents shall be mailed to MR for further publication and use

e. Dy.MR shall maintain a list of all approved documents in a 'Master List of Documents'

2. Review and update documents as necessary and re-approve documents

a. Any amendment to a controlled document even if it is a minor change or review of the document should follow version control process. This changes or review shall be updated in the Revision History appropriately. The older version should be archived by the owner of the document

b. MR and ISMS team shall jointly review all ISMS documents at least 7 days prior to each Internal Audit

c. If any change is required, MR shall incorporate such changes and mail the revised document to COO for his adequacy review

d. COO / MR shall approve / disapprove the document based on the adequacy review

e. The approved or reviewed document shall be shared with Dy. MR for further circulation

f. Approved documents shall be available to all employees on SGA portal SGA EASy (http://sgaeasy/application/#/login) as per defined document circulation. Documents classified as "Confidential Internal" will be available on SGA EASy

g. Dy.MR shall update the revision details of the approved document in the 'Master List of Documents'

5.4 Control of documented information

1. The updated versions shall be made available to the user immediately after any change / revision in the document
2. All documented information shall be protected from possible corruption, virus infection or any other threat that may result into loss or damage of the record
3. The System Administrator shall maintain periodic backup of all documented information as per the Backup and Recovery Policy
4. Before releasing any new document, the Dy.MR shall identify and record a distribution list as per the classification within the master list of documents
5. The MR shall further ensure that the documents are delivered only to the person(s) as authorized in the distribution list
6. All documented information shall be stored in specific folder as per the classification or the subject
7. All obsolete records / documents shall be kept in separate folder either named as 'archive' folder or 'old data' folder
8. Business Unit or Department will be responsible for maintaining the documents of external origin and ensure confidentiality, integrity and availability of the document

9. Once the controlled copy is printed, it is designated as uncontrolled. They are normally distributed to clients as per request depending on the document classification. External distribution is restricted by commercial considerations and these copies are not covered in the Procedure for Control of documented information
10. Retention time for all documented information shall be defined based on either of the following requirements:
    a. Statutory and regulatory requirements
    b. Customer specifications or contractual obligations
    c. Internal traceability requirements
    d. General requirements
11. Disposal of records / documents will be defined and followed by each business unit / department

6. References

1. Master List of Documents