Information Asset Classification & Handling Procedure

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_PR_Information Asset Classification & Handling Procedure_v2.0
Author	Smitha Saju
Reviewed By	Rohit Kalghatgi
Approved By	Rohit Kalghatgi
Owner	Rohit Kalghatgi
Document Type	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 guidance on:

1. Classifying information generated or used by SG Analytics and
2. Recommended ways to label, store, transmit, and dispose of such information, depending on its classification
3. Classifying IT Assets and systems so that appropriate controls can be implemented

1.2 Scope

This procedure shall be applicable to all information and IT assets within SGA.

1.3 Glossary of Terms

Terms	Description
BU	Business Unit
COO	Chief Operating Officer
Dy.MR	Deputy Management Representative
IT	Information Technology
MR	Management Representative
SGA	SG Analytics Pvt. Ltd.
UPS	Un-interrupted Power Supply

1.4 Definition

Asset: Anything that has value to the organization can be considered as an asset.

Information: Information is an asset which, like other important business assets has value to an organization and consequently needs to be suitably protected.

2. Responsibility

	Responsible	Accountable	Consulted	Informed
Identification and classification of IT assets	IT Team	Dy.MR	BU Lead	COO
Identification and classification of Information assets	MR	MR	BU Lead	COO
Labelling of assets	IT Team	Dy.MR	BU Lead	BU Lead

3. Procedure

3.1 IT Assets

Each IT asset of SGA handled by users and / or administrators, IT and the IT support staff will be classified and labelled either as critical or non-critical asset. Access control to these systems will adhere to the guidelines set in the access control policy - Logical.

3.2 Classification of IT Assets

Critical: The critical systems are classified as the systems:

a. Loss of which will result into loss of business or legal breaches or render an important business process or project disrupted for an unacceptable / long period

b. Which hold information about mergers / acquisitions; major trade secrets, strategic plans, financial results prior to release, individually identifiable medical records, client data, trade-controlled information, files containing clear-text passwords, digital certificate private keys, PIN or other confidential personal identifiers

c. Un-authorized access to which can cause severe harm e.g., severe legal or financial liability, extreme harm to competitive position; significant harm to company reputation

d. Unavailability of which can result into unavailability of systems classified above e.g. UPS, Generator etc.

Non-critical: All other systems those do not fall into any of the above categories.

Critical system within SG Analytics includes:

a. Cloud Applications

b. All core LAN and WAN network elements

c. Internet and WAN Links

d. Power supply to server / firewall room

e. Air-conditioning to server/firewall room

f. All laptops except those which are unassigned or maintained for allocation pool

g. Desktops – as may be identified by users/ projects from time to time

h. IP addresses

3.3 Asset Labelling and Handling

The assets shall be classified and clearly labelled so that all users are aware of the ownership and classification of the asset.

From the time when IT asset and non- IT asset is created until it is destroyed or de-classified, it must be labelled (marked) with a sensitivity designation.

Information and its related asset shall be processed and stored strictly in accordance with the classification levels assigned to those assets.

Access to the information assets shall be the responsibility of a designated owner or custodian.

3.4 Information Assets

The classification system set forth in these guidelines is intended to be simple and intuitive. Apart from information intended for public disclosure, Company information should be classified into one of three categories:

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.

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.
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 clients / vendors outside the organization

Label	Public	Confidential Internal	Confidential Sensitive	Confidential Limited
Examples	Press releases and company advertising (once approved for issuance); information on public portions of Company websites.	Company organization charts and telephone directories	Individually identifiable customer or client information / data; cost or pricing information; individually identifiable sensitive personnel information (e.g. compensation data), social security numbers, and credit card numbers.	Merger/acquisition-related information; major trade secrets; strategic plans; financial results prior to release; individually identifiable medical records; trade-controlled information; files containing clear-text passwords, digital certificate private keys, PINs, or other confidential personal identifiers.
Impact of Unauthorized Disclosure	No Harm	Limited Harm	Significant harm (e.g., legal or financial liability, adverse competitive impact, harm to Company reputation) Appropriate markings ("Confidential" or equivalent) strongly recommended Specific access restrictions (e.g.,	Severe harm (e.g., severe legal or financial liability, extreme harm to competitive position; significant harm to Company reputation)

Label	Public	Confidential Internal	Confidential Sensitive	Confidential Limited
			"For SG Analytics , Need-to-Know Use Only") also recommended	
Physical Labelling (Paper, Diskette or Tape Label)	None required	Appropriate markings ("Internal" or equivalent) recommended, but not required. Specific access restrictions (e.g., "For Internal SG Analytics Use Only") also recommended.	Appropriate markings ("Confidential" or equivalent) strongly recommended Specific access restrictions (e.g., "For SG Analytics , Need-to-Know Use Only") also recommended	Appropriate markings ("Restricted" or equivalent) required. Specific access restrictions (e.g. "For Use By Named Individuals Only") also recommended.
Electronic Labelling (Digital File, E-mail, or Web Page)	None required	Appropriate markings (as above) on subject-line or header/footer recommended, but not required.	Appropriate markings (as above) on subject-line or header/footer strongly recommended.	Appropriate markings (as above) on subject-line or header/footer strongly recommended.
Physical Storage (Paper, Diskette, or Tape)	No security requirements	Secure office or other location. Room need not be locked if access to the building or floor is restricted to SGA employees and authorized non-employees	Secure office or other location. Storage in a locked drawer, file cabinet, or office recommended, but not required.	Storage in a locked drawer, file cabinet, or office required. If stored in an open-file storage area, access to the area must be restricted to authorized personnel.
Electronic Storage (Digital File, E-mail, or Web Page)	No security requirements	Stored in a directory or folder with restricted access, e.g., password protection.	Information should be stored in encrypted form (using Corporate or business approved methods), unless your business does not provide such capability	Information should be stored in encrypted form (using Corporate or business approved methods), business does not provide such capability. Stored in a directory or

Label	Public	Confidential Internal	Confidential Sensitive	Confidential Limited
			Stored in a directory or folder with controlled access, e.g., password protection.	folder with controlled access, e.g., password protection.
Physical Transmission (Paper, Diskette, or Tape)	No security requirements	Internal SGA – No security requirements. External – Sealed envelope.	Appropriately marked, encrypt the content in case of Diskette or Tape or CD as per Cryptographic Policy and then sealed	Appropriately marked, encrypt the content in case of Diskette or Tape or CD as per Cryptographic Policy
Electronic Transmission (Digital File, E-mail, or Web Page)	No security requirements	Information should be transmitted to a verified account (email address or login ID).	Information should be transmitted in encrypted form (using Corporate or business approved methods), unless your business has determined that it does not provide such capability. Transmission should have controlled access, e.g., password protected account login.	Information should be transmitted in encrypted form (using Corporate or business approved methods) and addressee must be separately authenticated before access granted. Transmission should have controlled access, e.g., password protected account login.
Retention	To be decided by owner dependent on contractual obligation and compliance.			
Physical Disposal (Paper, Diskette, Tape, CD's or Hard Disks/ Drives)	No security requirements	After applicable Electronic Disposal, secure onsite or offsite physical disposal using Corporate or business approved methods for this	After applicable Electronic Disposal, secure onsite or offsite physical disposal using Corporate or business approved methods (for	After applicable Electronic Disposal, secure onsite disposal using Corporate or Information Disposal Policy for this data class. It is recommended

Label	Public	Confidential Internal	Confidential Sensitive	Confidential Limited
		data class.	example SLA with customer) for this data class. It is recommended to shred paper, break CD's and degauss magnetic media.	to shred paper, break CD's and degauss magnetic media. Disposal audit trail recommended.
Electronic Disposal (Digital File)	No security requirements	Removal of directory entry for file.	Removal of directory entry for file.	Removal of directory entry for file. File space should be over-written (using Corporate or business-approved methods) where possible.

4. Reference

None