Access Control Policy - Logical

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_Access Control Policy_Logical_v2.0
Author	Umed Patil
Reviewed By	Rohit Kalghatgi
Approved By	Rohit Kalghatgi
Owner	Umed Patil
Document Type	Policy
Document Status	Approved
Document Circulation	Confidential Internal
Document View Level	Internal
Release Date (dd-mm-yyyy)	18-01-2017

Revision History

Version	Date (DD-MM-YYYY)	Author (Designation: Name)	Changes (Short Description)	Remarks
v1.0	26-07-2016	Manager IT Umed Patil	-	Initial document
v2.0	18-01-2017	Manager IT Umed Patil	BUH / DH changed to BU Lead	Reviewed Document

Content

1. Introduction

1.1 Objective

The purpose of this policy is to protect against the unauthorised disclosure, modification, or destruction of the data residing in these systems, as well as the applications themselves. The users are responsible for protecting all SGA's information to which they are granted access. The access controls restrict access to system objects, such as files, directories, and devices based upon the identity of the user or the group to which the user belongs.

1.2 Scope

This policy applies to all employees and non-employees associated with SGA who access or administer access to information resources. This policy shall cover all IT systems, applications and IT resources owned by SGA.

1.3 Glossary of Terms

Terms	Description
BU	Business Unit
COO	Chief Operating Officer
ID	Identification
IT	Information Technology
OS	Operating System
USB	Universal Serial Bus
SGA	SG Analytics Pvt. Ltd.

2. Responsibility

The IT team will be responsible for verifying the effectiveness of the process and its revision whenever required.

3. Policy

1. The access to information and information processing facilities shall be controlled based on

   a. Business requirements

   b. Security requirements

   c. Asset Classification Policy

   d. Need-To-Do task basis

2. The formal Access Control Procedure – Logical shall be in place for granting and revoking access to all information systems and services

3. All the users to whom the access to Information system shall be provided shall register through the Helpdesk portal and approval from the BU Lead. Based on this the user shall be provided the access to information assets

4. SGA will ensure that all users have a unique identifier (user ID) for their individual use only. The use of group IDs will be permitted with prior authorization where they are suitable for the work carried out

5. IT Team provides the password to the user directly or via email to maintain its secrecy
6. Generic User-IDs shall exist for administrators of specific applications / systems only
7. OS level and Network level controls shall be established to protect un-authorized logical access to IT Infrastructure
8. The user shall be provided different user-ids to access different information systems. The control shall be established so that intruder shall not override system and application controls
9. IT shall be responsible to establish a secured procedure for logging into an operating system, application systems to minimize the opportunity for unauthorized access. Relevant audit features shall be enabled to establish accountability
10. A strong password policy shall be enforced through technical means to ensure password security
11. User access rights shall be reviewed at regular intervals. The access rights of user shall be immediately revoked on transfer / change of job or role
12. The access rights shall be only approved by SGA Account / Project manager for the concerned client
13. USB external storage device is blocked at organization level, any data to be copied on USB / external storage needs business justification & required to undergo approval process. Required data on USB / external storage should be validated by concerned account / project manager
14. SGA will exercise special care in allocation, reviewing of privileged IDs. Privileged IDs shall be different ID from those used for normal business use
15. All users shall ensure to protect sensitive or critical information on paper or electronic media and store them in lock and key
16. Wherever technically feasible, inactive sessions will shut down after a defined period of in activity
17. Use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled
18. The location, time and access control restrictions shall be established for critical application software to protect information security
19. While using sensitive application and when information i.e. Program (application), Data or output shall be protected with a restricted access, the system shall be isolated to protect sensitive information
20. Daily / Weekly / Monthly MIS reports highlighting the deviations flags will be generated by SGA' IT team

4. Procedure

4.1 Guidelines

1. The User ID (E-mail ID / ADS login ID) assigned to the individual will be as per the pre-determined naming convention as follows in descending priority:
   a. First name
   b. First name + First Character of Last name
   c. First name + Last name
   d. First Character of First name + Last name
   e. Name as per discussion with user
2. Network Operating System logon to domain /desktop through terminals shall be in a secure manner so as:
   a. Unattended user equipments such as desktops shall be locked and revoked with password
   b. Other equipments shall be controlled with appropriate protection.
3. All users shall store all the media and documents in lock and key to protect from un-authorized access.
4. All the confidential documents shall be immediately removed from printer, fax machine, scanner, and Xerox machines.
5. Department Head/ CEO shall revoke the privileges of a user under the following circumstances:
   a. Any conduct that is deemed as interfering with the normal and proper operation of the SG Analytics' information systems
   b. Any conduct that is deemed to adversely affect the ability of others to use the information systems
   c. Any conduct that is deemed to be harmful or offensive to others
   d. Termination of service/transfer of user
6. All User-IDs that have not been used for a specific period as defined in this procedure / guidelines shall be temporarily suspended and / or reset.
7. Wherever possible all secure login and logout controls provided with the operating system shall be configured to protect the security of Information system such as.
   a. Display a general notice warning that authorized users shall only access the system
   b. Limit the number of unsuccessful attempts and then shall be automatically locked
   c. On successful logon system should display and log details of last successful / unsuccessful logon