Access Control Policy - Physical

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 - Physical_v2.0
Author	Sandeep Datta
Reviewed By	Rohit Kalghatgi
Approved By	Rohit Kalghatgi
Owner	Sandeep Datta
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	Head - HR and Admin Sandeep Datta	-	Initial Document
v2.0	18-01-2017	-	-	Reviewed Document

Content

1. Introduction 5

1.1 Objective 5

1.2 Scope 5

1.3 Glossary of Terms 5

2. Responsibility 5

3. Policy 5

4. Guidelines 6

4.1 Do’s and don’ts 6

5. Non-adherence to the policy 7

6. Reference 7

1. Introduction

1.1 Objective

This policy addresses all the aspects involved in prevention of unauthorized physical access, theft, damage and interference to information and IT systems / assets, which lead to interruption of business activities.

1.2 Scope

This policy shall be applicable to EON premises of SGA.

1.3 Glossary of Terms

Terms	Description
Admin	Administration
IT	Information Technology
SGA	SG Analytics Pvt. Ltd.

2. Responsibility

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

3. Policy

1. The physical security in SGA shall be controlled by physical security in accordance with the procedure provided by the Head – Admin
2. The physical barriers shall be constructed around the business premises and the information processing facilities, depending on location requirements, to provide physical security
3. A list of all sensitive areas shall be maintained by the Admin team for monitoring purpose. Sensitive areas shall be defined and marked as follows:
    a. Restricted area: This shall be the area where 'Confidential' / 'Restricted' information is stored / processed

    b. Employee work area: This shall be the area where employees work and information classified , stored / processed
4. The visibility of the sensitive areas from outside the premises shall be avoided
5. A strict access control shall be established in the sensitive areas
6. SGA employees mapped with physical access card are allowed to enter in assigned client / project work area
7. Tailgating is strictly prohibited & treated as violation. Security guards are in place to restrict any tailgating or double entrant activities. Surveillance camera at the entry & exit points is used to identify tailgaters
8. Access to the offices will be strictly controlled, and visitors will be permitted access through the reception area only. SGA is equipped with video surveillance and security alarms, which is closely monitored by our security personnel at our reception desk. Movement of

equipment will be controlled by procedures operating under the Fixed Assets procedures of SGA

9. 'Restricted area' shall be protected from natural and man-made incidences such as fire, flood, civil unrest and man-made disaster
10. The delivery and loading areas pertaining to IT equipment's shall be separated from information processing facilities
11. An identification badge / access card shall be issued to all employees and non-employees (contractors and third party personnel) for access to SGA premises. All employees and non-employees shall visibly display the badges within SGA premises
12. Access to 'Restricted area' shall be controlled as per instructions from Head Admin
13. The equipment / IT assets which are classified as "Critical" shall be protected from environmental threats and hazards and un-authorized access
14. Any incidents related to physical security breach resulting in un-authorized access shall be escalated to Security for incident management
15. The power, telecommunication and data cabling shall be protected from interceptions and damages. The necessary distance between the power and data cables shall be maintained to protect the data loss in transit
16. The equipment's shall be maintained periodically to ensure its continual availability and integrity
17. All the equipment's and media shall be taken off-site with proper authorization and record to this effect shall be maintained in material inward / outward register
18. Any media or device shall be checked to ensure that any sensitive data and / or licensed software on it are securely overwritten prior to disposal
19. IT assets will be maintained and controlled by the IT team
20. The incoming / outgoing IT material shall be checked and registered by the Admin team

4. Guidelines

1. The employee needs to ensure that the green light blinks while swiping the access card, especially for the first and the last swipe, to avoid any discrepancy in salary calculations
2. Employees should carry their access cards if working on weekly holidays or public holidays
3. The employee should ensure that the access door and bay door should be closed during entry or exist
4. All visitors to the premises will be issued with visitor badges at the reception. The visitor badges must be displayed at all times within the premises. The visitors should be escorted by their respective employees at all times. The visitors will remain at the reception desk until an appropriate member of staff is available to escort them in and out of the office area

4.1 Do's and don'ts

1. Only authorized people are allowed to enter the employee work area

2. Do not smoke inside office and building premises or near secure area
3. Computers and internet to be used only for official purpose
4. Lock your machine while leaving it unattended
5. Use email, internet, network resources and printers judiciously
6. Keep the access doors closed

5. Non-adherence to the policy

1. If an employee forgets to bring his / her access card, a temporary card can be obtained from the reception desk by entering the details in the register maintained. Employees need to share their temporary identification card number to time@sganalytics.com
2. If employee forgets to bring his / her access card, starting from 2nd instance (allowing 1 lapse per month), he / she will be levied a charge of INR 200 per instance
3. Employees need to use the access cards at all doors. Tail-gating is strictly prohibited. If any employee is found guilty of such behaviour by the Admin team or Security, an email will be sent to the employee, respective Manager and time@sganalytics.com. A penalty of INR 500 per instance will be levied for any non-compliance
4. Any penalty amount will be deducted from the employee’s current month salary

6. Reference

None