Solve.
Synergise.
Surpass.

SG Analytics

Wi-Fi Network 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.

Solve.
Synergise.
Surpass.

Document Summary

Document Reference #	SGA_PO_Wifi Network Policy_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

Solve.
Synergise.
Surpass.

SG Analytics

Revision History

Version	Date (DD-MM-YYYY)	Author (Designation: Name)	Changes (Short Description)	Remarks
v1.0	21-07-2016	Manager IT Umed Patil	-	Initial document
v2.0	18-01-2017	-	-	Reviewed Document

Solve.
Synergise.
Surpass.

Content

Solve.
Synergise.
Surpass.

1. Introduction

1.1 Objective

This policy shall control the use of Wi-Fi network in SGA to prevent violation of security rules and its misuse.

1.2 Scope

This policy shall be applicable to all employees of SGA and guest laptops or smart phones.

1.3 Glossary of Terms

Terms	Description
ISMS	Information Security Management System
IT	Information Technology
MR	Management Representative
SGA	SG Analytics Pvt. Ltd.

2. Responsible

IT Head will be responsible for verifying the effectiveness of this policy.

3. Policy

1. IT team shall ensure that only verified and authorized computers, laptops, and other portable systems can use Wi-Fi network

2. Use of secure Wi-Fi network shall be prohibited for unauthorized use and system

3. Service request management process shall be adopted by IT department to assign Wi-Fi network use

4. IT team shall periodically check list of approved users for respective Wi-Fi networks

5. IT team shall share incidents related to misuse of Wi-Fi networks with MR

6. Only SGA laptop / asset will have Wi-Fi access to SGA Corporate network

4. References

1. ISMS Manual

2. Internal Audit Procedure

3. Information Security Risk Management

4. List of authorized users of different Wi-Fi networks