Acceptable Use 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.

Document Summary

Document Reference #	SGA_PnP_Acceptable Use Policy_v1.0
Author	Umed Patil
Reviewed By	Rohit Kalghatgi
Approved By	Rohit Kalghatgi
Owner	Umed Patil
Document Type	Policy and Procedure
Document Status	Approved
Document Circulation	Confidential Internal
Document View Level	Internal
Release Date (dd-mm-yyyy)	19-01-2017

Revision History

Version	Date (DD-MM-YYYY)	Author (Designation: Name)	Changes (Short Description)	Remarks
v1.0	19-01-2017	Manager IT Umed Patil	-	Initial document

Content

1. Introduction 5
   1.1 Objective 5
   1.2 Scope 5
   1.3 Glossary of Terms 5
2. Responsibility 5
3. Definition 6
4. Policy 7
   4.1 Computing Devices 7
   A. Employees 7
   B. Non-employees / Visitors 7
   C. Loss of Computing Device 7
   4.2 Storage Media 8
   4.3 Electronic Messaging 8
   4.4 Desk phone & Mobile 9
   4.5 Copiers & Printers 10
5. Procedure for Computing Devices and Storage Media 10
   5.1 Description 10
   5.2 Physical Security 10
   5.3 Data Security 10
   5.4 When Travelling 11
   5.5 Guidelines 11
   5.6 Network Security 11
6. Violation 12
7. Reference 12

1. Introduction

1.1 Objective

This policy defines the acceptable use of SGA's Information Processing Infrastructure which includes computing devices, storage media, communication media etc. This policy further prescribes the roles and responsibilities of all employees, contractors, third party personnel of SGA.

1.2 Scope

This policy shall govern use of all computing devices, storage media, electronic messaging services, desk phone & mobile, and copiers & printers by employees, contractors, third party personnel of SGA.

1.3 Glossary of Terms

Terms	Description
Admin	Administration
BUH	Business Unit Head
CD	Compact Disc
COO	Chief Operating Officer
DH	Department Head
DVD	Digital Video Disc
Dy. MR	Deputy Management Representative
FIR	First Information Report
HDD	Hard Disk Drive
HR	Human Resource
IDS	Intrusion Detection System
IT	Information Technology
MAC	Media Access Control
MR	Management Representative
PDA	Personal Digital Assistant
SGA	SG Analytics Pvt. Ltd.
USB	Universal Serial Bus

2. Responsibility

Category	Responsible	Accountable	Consulted	Informed
Computing Devices – Physical Security	Respective User	Respective User	IT	MR
Computing Devices – Data Security	Respective User/ System Administrator	Respective User / IT Head	MR	COO

Category	Responsible	Accountable	Consulted	Informed
Removable devices	Respective User/ System Administrator	Respective User / IT Head	MR	COO
Network Security	IT	IT Head	COO	COO
Computing Device usage by Third Party	BUH / DH	BUH / DH	MR	COO
Electronic Messaging	Respective User	Respective User	IT	MR
Copiers / Printers	Respective User	Respective User	Admin	MR
Desk Phone / Mobile	Respective User	Respective User	MR	COO

3. Definition

1. Computing devices would include but are not limited to:
   a. Laptops / Desktops
   b. PDA / Tablets / Notebooks / Mobile / Smart phones
   c. Pocket Computer
   d. iPods
   e. Fax machine
2. Storage media would include but are not limited to:
   a. USB / Zip / Pen / Flash Drive
   b. Memory Cards
   c. CD writers / DVD / Blue Ray Disks
   d. Tape and Cartridges
   e. Digital Camera / Web cam
   f. Hard drive / HDD
   g. Smart phone storage
3. Host based firewalls: Host based Firewall (e.g. Windows or OS Firewall) protects computer by blocking communications that might actually be dangerous software trying to find a way to connect to your computer, rather than communications from a person or program you

want to interact with. Such firewalls keep mobile computers protected from constantly changing internet threats.

4. Policy

4.1 Computing Devices

A. Employees

1. Each employee has an affirmative obligation to safeguard the hardware, software and data processed by SGA computers against damage, alterations, theft, fraudulent manipulation, unauthorized access, and unauthorized disclosure of proprietary and confidential information
2. Access to data on any computing devices through SGA network shall be as per Access Control Policy – Logical
3. Employees are restricted to use personal laptop within the SGA premises
4. While issuing desktops / laptops to employees, SGA pre-configures rules and protocols into the desktop / laptop hardware, which ensures acceptable use of the device
5. SGA has an absolute right to monitor, limit and control the configuration and use of its computer systems and networks

B. Non-employees / Visitors

1. Visitors / non-employees can be allowed only to carry computing devices inside the premises in accordance with the procedure mentioned below:
   a. All the computing devices shall adhere to well defined procedure and can be in SGA premises with prior permission of IT team and MR
   b. The prior approval from the respective personnel whom to meet shall be required, to use computing devices inside SGA for demonstration purpose only
   c. Contractors and Third party's computing devices shall not be allowed to connect to SGA's Corporate network
   d. For specific case, SGA will provide only isolated Wi-fi access within the premises subject to proper justification

C. Loss of Computing Device

1. In case an employee misplaces a company provided computing device, the employee must immediately report the loss to Admin, IT and respective Manager
2. The employee must lodge a FIR to the relevant law enforcement agency. Finally, the employee will need to provide a new / similar condition computing device to the company
3. Alternatively, an employee has an option to let SGA procure a new computing device and deduct the cost of the device from his / her salary
4. SGA reserves the right to conduct an inquiry on the circumstances in which the computing device is lost and to take an appropriate action as per Disciplinary Action Policy in case the employee is found at fault

4.2 Storage Media

At any given point in time, no employee or contractor or visitor shall be allowed to carry any storage media within SGA's premises or connect to corporate network.

SGA's IT team is responsible for issuing computing devices to employees with configuration that disables all USB / HDMI ports and are equipped with Data Leak Prevention (DLP) software, backup agent and antivirus software.

4.3 Electronic Messaging

1. A unique e-mail address shall be provided to each employee of SGA who needs to communicate through e-mail for direct or indirect benefit of SGA
2. E-mail address shall be provided to non-employees at complete discretion of SGA's management
3. It is the responsibility of the sender to validate the recipient's authenticity
4. All the information created, sent, or received via SGA's, e-mail system including e-mail messages, data and electronic files, **is the property of SGA**; employees shall have no exception of privacy regarding this information
5. SGA reserves its rights to:
   a. Deny an e-mail address to any individual or any team
   b. Allocate e-mail address as per Management and IT's discretion. The users will not have choice to decide their e-mail address
   c. Access, read, review, monitor, copy, intercept, block or auto forward e-mails and files on its system for legitimate business reasons, without prior notice
6. When deemed necessary, SGA reserves the right to disclose text or images to law enforcement agencies or other third parties without the employee's consent
7. The electronic messages shall be protected from un-authorized access, alteration and denial of service
8. The sender shall be responsible for ensuring that documents and messages are not sent to a wrong email address or by using a wrong stored id
9. The users must also abide by copyright laws, ethics rules, and other applicable laws while using SGA's e-mail service
10. The users shall exercise sound judgment when distributing messages
11. The user shall not use e-mail service for un-authorized use. Unauthorized use of email system shall mean:

    a. Transmitting and/ or distributing e-mail containing derogatory, inflammatory, insulting, abusive information about any other SGA employee, client, associate or any other person whatsoever

    b. Conducting any business (whether personal or professional) via SGA e-mail system other than legitimate SGA business

c. Overloading unnecessarily or frivolously the e-mail system (e.g. chain mail, spamming, executable graphics and/or programs and junk mail which is not allowed

d. Enclosing information that is harmful to SGA or members of SGA

e. Sending or distributing questionable e-mail containing expletives or pornography

12. The e-mail attachments with extensions such as ".exe", ".scr", ".vbs" & ".vir" etc. will be blocked for security reasons
13. The e-mail re-direction / auto-forwarding from SGA - e-mail address to any non-SGA e-mail address is strictly prohibited
14. SGA employees cannot share emails to any personal domains such as **gmail.com**, **yahoo.com**, **outlook.com** etc.
15. E-mail users should protect others' right to confidentiality
16. The use of SGA's e-mail service to solicit for any purpose, commercial, personal or otherwise, without the consent of the SGA, Management is strictly prohibited
17. Users shall report email security incidents in accordance with the Information Security Incident Management Procedure
18. Impersonation of other employees is forbidden
19. No employee may load or allow others to load any software of any kind, including freeware or shareware or any copyrighted material, on any SGA computing system without prior approval
20. Voice and video access communication is provided to employees with appropriate business justification and through approval process
21. Employees are restricted to delete any business critical emails. While serving the notice period, IT team has the right to actively conduct surveillance of their emails. During handover if IT team observes any critical emails are deleted, SGA reserves the right to conduct an inquiry and may hold all financial transaction till such time
22. The email attachment limit is 7MB
23. Mailbox not accessed for 90 days will be subject to cancellation
24. SGA's IT team will be responsible for storing all information in an encrypted format using AES encryption algorithm. SGA uses SSL and TLS protocol for outbound SMTP (email) services

4.4 Desk phone & Mobile

1. The employee shall report in case they suspect any interception or misrouting of information exchanged through phone or mobiles. The employee shall report to Dy.MR.
2. It's is the responsibility of the employee to validate the recipient's authenticity
3. The employee shall take appropriate precautions, e.g.:
   a. not to reveal sensitive information to avoid being overheard or intercepted when making a phone call

b. people in their immediate vicinity particularly when using mobile phones;

c. wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers;

d. people at the recipient's end

4. The employee shall not have confidential conversation in public places or open offices, elevators and meeting places with non-sound proofed-walls

5. The employee avoid usage of client names in public places, elevators or open offices

6. In case an SGA misplaces a personal wireless communication device which has official emails configured on it, an employee must immediately report the loss of the device to IT team

4.5 Copiers & Printers

1. The user shall be responsible for not leaving sensitive or critical information on printing facilities eg: copiers and printers
2. The user shall pay attention to the fact that the modern copiers have page, caches, and stored pages in case of a paper fault, which will be printed once the fault is clear. Hence it is the user's responsibility to make sure that such prints do not land up in unauthorized hands

3. It is sender's responsibility not to leave documents unattended after a facsimile transmission

4. The user of facsimile machine shall ensure that documents and messages are not stored in the memory of the machine after the use is over

5. Procedure for Computing Devices and Storage Media

5.1 Description

As per SGA Information Security Policy, employees shall be responsible for the acceptable usage of computing and storage devices facilities such as notebooks and laptops for business purposes. This document provides basic security guidelines to SGA users while using laptop, desktop & desk phones and mobile phones in case SGA email system configured. Use of any storage media such as USB, Memory Card, CD, DVD, Blue Ray Disk, Tapes and Digital Camera is strictly prohibited.

5.2 Physical Security

1. Laptop shall be transported in a sturdy, weatherproof, padded, adequately sized bag

2. Laptop / Desktop shall never be kept unattended. It must be assured that it is locked and secured anytime the user is away from his / her desk

3. Laptop shall not be positioned near an exterior window, where it would be subject to a smash and grab type theft

4. The make, model, and serial number of the computer and any peripherals shall be recorded in the asset inventory

5.3 Data Security

1. All important data shall be backed up and the current copies kept readily available. Back up shall be done on appropriate media by the owner of the asset with the help of IT

2. Programs shall be quit prior to shutting down of the laptop to avoid data loss and program corruption
3. The hard disk shall never be formatted without prior testing of information that is backed up
4. All USB ports are disabled
5. Antivirus program with the latest possible virus updates shall be installed (configured for auto updates). The program will be configured for real time protection, to retrieve updates daily, and to perform an anti-virus or malware scan at least once a week
6. To add a layer of protection to the laptop, a host-based personal firewall product or IDS with latest possible updates shall be installed. The program will be operational every time to protect the computer from worms and other malware, whenever the computer is connected to any un-trusted network including the internet
7. Additional malware protection software will be active on laptops in accordance with the Malicious Code Policy

5.4 When Travelling

1. Care shall be taken not to forget / misplace the laptop and thus prevent loss
2. The equipment shall not be kept unattended or out of sight, even during a security check at an airport
3. The laptop shall not be checked in as baggage
4. When travelling out of country, a proper documentation shall be carried to ensure easy passage

5.5 Guidelines

1. The users will not be allowed to have administrative rights on computing devices, unless the COO grants special authorisation
2. The user agrees not to use the computing devices for personal use
3. Laptop/smart phone owned by SGA or allowed on SGA's network must be identified by their MAC address by the IT department before connecting to the network
4. The device must meet the computer connection standards described in the following section
5. The user must be identified by name and contact information to the IT department
6. Devices not owned by SGA are subject to software audit; to ensure that no software is loaded that pose risks to the network security. All computing devices are subject to software audit at any time
7. Access rights to SGA's network cannot be transferred to another person, even if that person is using an allowed computing device

5.6 Network Security

Computing device entering the network will meet the following requirements:

If the computing device is owned by SGA and used regularly by employees, then the device will be checked according to that part of the policy.

1. Determine whether the anti-virus program is up to date, has the latest virus definitions, is configured properly, and is running properly. If it fails one of these conditions or has not been scanned for a virus within the last week, a full virus scan must be done before the computing device can be used in network
2. Test the device and scan for additional malware such as adware or spyware test to determine whether the device has a worm
3. Test the state of stored sensitive data to ensure that it is protected
4. Remove any malware on the device, if detected. Information about any malware found shall be logged

6. Violation

Any violation of this policy will subject a user to disciplinary action as per Human Resource Procedure.

7. Reference

1. Access Control Policy – Logical
2. Information Security Incident Management
3. Disciplinary Action Policy