The purpose of this document is to outline the security procedures that are enforced within Survey Analytics. The procedures stated here are applicable to all employees of Survey Analytics. There will be no exceptions made to this policy under any circumstances. Any employee found violating this policy will be terminated immediately and access will be revoked.

1. Network Access

a. User Identification and Passwords

i. Each user is allocated an individual user name and password. Logon passwords must not be written down or disclosed to another individual. The owner of a particular user name will be held responsible for all actions performed using this user name.

ii. Staff must notify the IT Help Desk when moving to a new position or location within Survey Analytics. This ensures that the necessary setups to provide fast access to the most appropriate mail and file servers can be put in place.

iii. Management must notify IT of staff changes that might affect security. An example of this would be an individual who has access to restricted confidential client information and moves to another role where this access is not required.

iv. All user accounts have the following password settings:

1. Minimum password length of 8 characters;
2. A combination of alpha, numeric and punctuation should be used;
3. Users are forced to change their passwords every (insert number) days;
4. Users cannot repeat passwords;
5. Accounts are locked after (insert number) incorrect login attempts.

v. Passwords must not be easily guessed (i.e. names, months of the year, days of the week, usernames, etc. must not be used as passwords).

b. Access to Survey Analytics Information

i. All information held on the networks including email, file systems and databases are the property of Survey Analytics and staff should have no expectation of privacy for this data.

ii. Although it is not the general practice of Survey Analytics to monitor stored files, email messages and Internet access for their general content, Survey Analytics reserves the right to do so for the protection of staff, for system performance, maintenance, auditing, security or investigative functions (including evidence of unlawful activity or breaches to Survey Analytics policy) and to protect itself from potential corporate liability.

iii. Requests to access the computer account of a member of staff who is absent from the office must be directed to the IT Help Desk/relevant IT resource in writing by the "Relevant Manager". The access is given effect by changing the user's password and allowing the "Relevant Manager" or a colleague to access the account directly. Where this access is granted it must be used for enquiry purposes only.

iv. Staff must not issue any information to third parties unless they have authorisation to do so.

v. Users are only permitted to access electronic information and data that they require to perform their duties.

vi. If confidential information is lost, either through loss of a notebook computer, backup media or other security breach, the IT Help Desk/relevant IT resource must be notified immediately.

vii. All computers must be switched off at the end of the day. This action erases residual information contained in the computer's memory and assists with overnight anti-virus software updates.

c. Personal use of computer systems

i. While Survey Analytics PCs and notebook computers are provided for business use, it is acceptable to use them for a limited amount of personal use. This limited personal use of PCs is permitted provided such use does not a) interfere with the user's job commitments; or b) have a detrimental effect on the computer or network's performance.

ii. Staff must not use Survey Analytics systems or the Internet for commercial activities that are not related to the business of Survey Analytics.

d. PC and Notebook Security

i. General

1. PCs and notebook computers must not be left unattended for long periods while signed-on e.g. during lunch, coffee breaks etc. Users must either logoff or activate a password-controlled screensaver if they are leaving their PC. The screensaver should be set to activate by default after 10 minutes of inactivity.

2. IT equipment must not be removed from Survey Analytics premises unless written approval has been received from the IT Department/relevant IT resource. An exception is made for authorized off-site back-ups providing they are adequately protected against unauthorized access. All notebooks must be signed for before being removed from Survey Analytics premises. .

ii. Software

1. Software must not be copied, removed or transferred to any third party or non-organizational equipment such as home PCs without written authorization from the IT Department.

2. Only software that has been authorized by the IT Department may be used on PCs and notebook computers connected to the Survey Analytics IT network.

3. Downloading of any executable files (.exe) or software from the Internet is forbidden without written authorization from the IT Department/relevant IT resource. Staff may be given this authorization based on their specific job requirements.

iii. **Confidentiality**

1. Confidential data held on computer media (e.g. floppy disk) must be stored securely when not in use.

2. PCs and notebooks for disposal must have the hard disk 'wiped clean' before they are distributed outside Survey Analytics

2. DATA BACKUPS

a. The IT Department must take regular hot and backups of all production servers.

i. **Hot Backups**

1. A hot backup will be taken daily, weekly, and monthly that will be available for restore within 2 hours [Internal SLA].

2. Hot backups will be available only to system administrators and only for the purpose of a system restore. Under no circumstances will the backups be removed from the server or taken offsite.

ii. **Offline Backups**

1. Rotating offline backups will be executed weekly and monthly and stored to tape. These backups will be taken to an offline storage facility. In case of a catastrophic event, these tapes must be retrievable within 24 hours. [External SLA]

2. Survey Analytics has a contract with IRON Mountain to handle offline data backup storage. IM’s OffSite Tape Vaulting solution is responsible for handling the data pursuant to the same Data and Security policies of Survey Analytics or stricter.

3. Customer data shall never leave the Data Center for any other purpose other than off-site storage for backup.

b. Users must always save data and files on the network as opposed to the local hard disk. This ensures that regular backups are taken and are available for recovery purposes. Users should be aware that data saved on the local hard disk is not backed up by the IT Department/relevant IT resource.

3. USER IDENTIFICATION AND PASSWORDS

a. All unused usernames must be deleted following an initial period when they are disabled. Managers must inform the IT Help Desk/relevant IT resource when staff leave Survey Analytics to ensure that their usernames are promptly removed.

b. Staff transferring sections within Survey Analytics must have their access privileges reviewed and altered based on their new responsibilities, following notification to the IT Help Desk/relevant IT resource by the person moving location.

c. Usernames must conform to the standard Survey Analytics naming convention. The convention must be used consistently across all applications and platforms.

d. When the IT Help Desk/relevant IT resource are unsure of the identity of the user requesting a password change, then authorization must be received from relevant manager before the request is completed.

e. Survey Analytics hardware and software must have the vendor-supplied default passwords changed on installation. This applies to test as well as live environments.

4. IT Security Responsibilities

a.All unused usernames must be deleted following an initial period when they are disabled. Line managers must inform the IT Help Desk/relevant IT resource when a staff member leaves Survey Analytics to ensure that their usernames are promptly removed.

b.Staff transferring sections within Survey Analytics must have their access privileges reviewed and altered based on their new responsibilities, following notification to the IT Help Desk/relevant IT resource by the person moving location.

c.Usernames must conform to the standard Survey Analytics naming convention. The convention must be used consistently across all applications and platforms.

d.When the IT Help Desk/relevant IT resource are unsure of the identity of the user requesting a password change, then authorization must be received from relevant manager before the request is completed.

e.Survey Analytics hardware and software must have the vendor-supplied default passwords changed on installation. This applies to test as well as live environments.

f.Threat Management

i. Threats that are identified must be assessed within 24 hours [internal SLA] and an action plan set in place. If action is required, (moderate or high threat level) a solution must be implemented within two weeks [internal SLA].

g.Planned outages for maintenance activities must be scheduled and notified to all Enterprise and Community level subscribers.

h.Access logging will be enabled at the OS and Middleware level on all systems so that a consistent audit trail can be re-created.

i.All computer and network systems must be configured with UPS backups.

5. Third Party Access

a.Third Party Access can be defined as "The granting of access to Survey Analytics IT resources or data to an individual who is not an employee of Survey Analytics.

b.Examples of third parties include:

i. Software vendor who is providing technical support;

ii. Contractor or consultant;

iii. Service provider; and

iv. An individual providing outsourced service to Survey Analytics requiring access to applications or data.

c.Third Party Access can only be provided after the Third Party has signed a confidentiality agreement that must be included in their formal contract with Survey Analytics. Survey Analytics staff must never permit another individual to utilize their user name to access the Survey Analytics network.

d.Further requirements for granting Third Party Access are:

i. Risk analysis process;

ii. Approval by Data Owner;

iii. Approval by the Head of IT/relevant IT resource;

e.Third party access will only be permitted to facilities and data which are required to perform specific agreed tasks as identified by Survey Analytics.

f.Third party access will be audited randomly twice a year for security violations, improper use, and assessment of need.

6. IT Employee Screening

a.All employees will be screened via a criminal background check by a third party entity in addition to standard HR screening procedures (ie., employment verification, credit reference, etc).

7. Data Center Access

a.Physical access to servers in the data center will be restricted to IT administrators only.

b.The Data Center will be monitored 24 hours a day, seven days a week.

c.Visitors are not allowed – no exceptions.

d.IT managers must provide security personal with an updated access list to the data center. [managed by Internap Networks]

8. Data Handling Policy & PII Security Requirements

a. All Customer data is always stored in the data-center.

b. Customer data that is downloaded into PC's of SurveyAnalytics's support and administrative staff must be deleted from local machines (PC's, Mac's) within 24 hours. In cases where data is downloaded for a longer period of time - supervisors must be made aware of such and justification should be provided.

c. Under no circumstances, customer data should be downloaded into employees or contractors' unauthorized PC's.