Security and Reliability Statement

December 2018

***Confidential* - do not duplicate or distribute without written permission from SurveyShack (SSL) Ltd.**

This document describes the security environment and data management culture and processes of SurveyShack (SSL) Ltd.

We constantly strive to ensure the information contained herein is always accurate but because our security and data management processes evolve and adapt continuously to constantly changing conditions, this document may not always reflect our exact architecture and may therefore not always be error free. We reserve the right to modify this information at any time.

Questions or comments, please contact us on: admin@surveyshack.com

1 What does the statement cover?

SurveyShack (SSL) Ltd provides three main online-based services, including:

1.1 Online Solutions

All dedicated online solutions, including our 360 degree feedback tools, Performance Management tools and various other custom online solutions which are developed, hosted and supported in our cloud-based server environment.

1.2 SurveyGizmo Online Survey Tool Licenced Accounts

As a Certified Reseller of SurveyGizmo licensed accounts, SurveyShack (SSL) Ltd administers all new account subscriptions, annual renewals, accounts receivable and provides tier 1 user support for our SurveyGizmo Online Survey Tool subscribers.

1.3 Managed Survey Services

Our expert team of project managers undertake feedback-based projects to our clients' requirements. These projects are carried out using either our in-house managed survey services dedicated SurveyGizmo account, or an in-house Online Solution. All Managed Survey Service security and reliability requirements can be considered to be covered under either of points 1.1 and 1.2 above therefore.

2 General

SurveyShack acquires and manages data on two levels:

- Data acquired and managed in support of running our business (e.g. our own accounting, sales and marketing activities)
- Data acquired and managed on behalf of our customers (e.g. our customer's mailing lists and survey data)

*As an organisation therefore we act as both a **data controller** and a **data processor.***

2.1 Protection and Security of Data

Good information handling makes good business sense and as both a data controller and a data processor, SurveyShack takes our data security and protection responsibilities very seriously.

As has been described throughout this document, our responses to the ICO (Information Commissioner's Office) data protection checklist below confirms our sound knowledge and understanding of the requirements for data protection, as follows:

- Do we have a record of what personal and/or business data we hold and do we know what we use it for? **YES** ✓
- Do our customers know we have their personal and/or business data and understand how we use it? **YES** ✓
- Do we only collect the personal and/or business data we need? **YES** ✓
- Do we only keep personal data and/or business for as long as it is needed? **YES** ✓
- Do we keep personal and/or business data accurate and up to date? **YES** ✓
- Do we keep personal and/or business data secure? **YES** ✓
- Do we have a way for people to exercise their rights regarding the personal and/or business data we hold? **YES** ✓
- Do all of our staff know our data protection responsibilities? **YES** ✓

2.2 Registration

SurveyShack (SSL) Ltd is a ICO registered data controller (reg no: ZA288963).

2.3 Data Classification and Ownership

- As a **data controller**, all data acquired on behalf of our customers belongs to them. Our customers have complete and exclusive control over how their data is acquired, stored, shared and deleted.
- As a **data processor**, any data acquired and used as part of the running of our business is managed strictly in accordance with all relevant legislation and guidelines.

2.4 Security Control Policies and Procedures

All aspects of our system and data security processes and policies are documented and practised by all staff, subcontractors and stakeholders. Related policies include:

- Privacy Policy: https://www.surveyshack.com/privacy-policy/
- General Terms and Conditions: https://www.surveyshack.com/policies-terms-and-conditions/

2.5 Staff, Subcontractors and Third Parties

- All employees are subject to background verification checks prior to confirmation of their employment
- All staff, subcontractors and where necessary, third parties are required to sign a NDA or Confidentiality Agreement as a condition of employment or engagement to protect SurveyShack and/or customer information
- All staff and relevant subcontractors are trained, tested and regularly re-tested on their understanding of SurveyShack's policies and procedures to ensure they will always act in compliance with these
- All staff and subcontractors are immediately updated with all new/updated policy and procedural documentation
- All staff and subcontractors are aware of their responsibilities for leaving unattended equipment in a secure manner at all times
- Upon termination, all company-owned equipment is recovered and all access to company and/or client data is immediately revoked via centrally administered login access controls

2.6 Data Loss/Leakage

Any suspected or known loss or leakage of data is immediately reported to our data compliance manager. Where the significance of the issue warrants, this is reported to the client and if required also, the ICO, within the required maximum period of 72 hours.

2.7 Data Encryption

In all instances, any data transmitted electronically via the internet, via any transfer means (email or system user interface), is fully encrypted by means of SSL with 128 bit encryption (High) or RSA with 1024 bit exchange.

2.8 Network Security

As an organisation, SurveyShack does not utilise any form of organisational network. All business process related connections to the internet are made via unique local device browser sessions under strictly, centrally controlled username and password policy. All devices and connections made therefore follow DCHP IP address rules.

2.9 Business Continuity

Wherever possible, SurveyShack utilises proven, reliable internet cloud-based business process tools to administer and store all data and code. This ensures that all business-critical information and systems are:

- able to be accessed via multiple channels from any location worldwide
- available on a constant and permanent basis
- centrally managed and administered by the required authorised staff
- protected by best-in-practice security processes
- fully backed up and recoverable
- compliant with all relevant data protection and privacy requirements

As there is no dependence on any form of dedicated network, hardware or unique software to maintain business continuity, should it ever be required that any business-critical and/or client data may need to be recovered in the event of disaster or any form of unforeseen circumstance, this can be achieved virtually instantaneously. All members of the senior management team have been trained and are able to access all of our systems and processes at any time.

2.10 Disaster Recovery

See 2.9, 3.7 and 3.11

2.11 Disposal of Hardware

Should it ever be necessary to dispose of hardware which is capable of storing, and which may have ever stored personal and/or business related data, this is disposed of in accordance with environmental policy having first undergone permanent physical destruction of the storage media contained within the hardware unit.

3 Online Solutions Security

SurveyShack develops, builds and hosts numerous online solutions ranging from one-off, bespoke and highly custom 'Reportal' tools which provide time-saving automation to regular feedback and reporting tasks, through to multi-tenant software-as-a-service (SaaS) systems.

In all instances, system and data security, and reliability is the lifeblood of our business which we therefore take extremely seriously. The following should describe and reassure on our relentless pursuit of the best-practice approach to ensuring our systems are always as secure and reliable as is technically and humanly possible.

3.1 Overview

SurveyShack's online solutions are based on the tried and true LAMP (**Linux, Apache, MySQL and PHP**) combination of web-based development components. PHP code is written within the **Laravel** framework to ensure our tools keep pace with the latest in development methods, system security and version control, and to allow for the widest possible development tools integration options.

3.2 Cloud Infrastructure

All Unix (Linux) cloud servers are established strictly within the EU and are based on either a Ubunto or Debian OS. Apache service provides for webserver domain control.

3.3 Identity and Access Management

Access to server and the database is only possible via secure SSH (hashed) and centrally revocable keys which are placed on individual devices authorised to access the server only. It is not possible to gain access via the root at all.

3.4 Application Security

As well as strict server and database access control, Encryption of all movement of data within the database/code relationship of the system is provided for by PHP Data Objects (PDO) within the Laravel framework to mitigate against SQL injection risks.

3.5 Client User Password and IP Restriction Security

All client system user passwords are fully encrypted and set by users only. Very clear and strict password rules are applied including regular automatic password expiry and resets, long and detailed passwords, etc. In some instances, IP restrictions have been applied at server level permitting only IPs authorised by the client themselves to access the applications.

3.6 Anti Malware

Multiple security and malware detection, alerting, quarantining and reporting applications are in permanent use.

3.7 Change Control and Configuration Management

All code is repository-based (Bitbucket) which provides for effective version control, ease of update and rapid restoration if required

3.8 Penetration Testing

Penetration testing is able to be carried out upon request and at the client's expense

3.9 Physical Security

The SurveyShack server farm is hosted with a leading European Cloud service host in a locked cage-type environment where access to the server is restricted by secure appointment and photo ID security card access.

3.10 Host Security

Hosting is on a UNIX platform which has been hardened against attack by the following means:

- All currently available patches for OS, web servers and databases are constantly updated as soon as they are released
- Passwords for access to the server must follow these rules:
  - Must be a minimum of 8 characters long
  - Must have at least 1 English capital letter, 1 English lower case letter, 1 number and 1 alpha-numeric or "special" character o May not contain any full part of any employees email address, or full name
  - Must be changed at least every 45 days
  - Must not be the same as any of the past eight passwords used
  - Must not contain any common word in the dictionary or slang.

3.11 System and data Back-up

All databases and data are backed up on and off-server on an hourly (retained for 24hours), daily (kept for 24 hours) and weekly basis. See 3.7 above for a description of code version control and restoration.

4 Online Solutions Performance and Reliability

4.1 Uptime

Our target uptime is 99.9% which when excluding planned downtime and unplanned external internet failures beyond our control, we have been able to achieve consistently to date.

4.2 System User Support

All SurveyShack systems and services benefit from UK-based email user support during normal working hours. All incoming support requests are immediately logged, acknowledged and prioritised as follows:

- *Low:* Resolution as soon as possible
- *Normal:* Resolution within 24 hrs wherever possible

- *High:* Resolution within the same 12hr day wherever possible
- *Urgent:* Resolution within 2 hrs or sooner

User support can be requested using the 'Help' option provided for within most of our online solutions, or directly via our *support@surveyshack.com* email address.

5 SurveyGizmo Online Survey Tool Licenced Accounts

5.1 Overview

Having over 17 years of experience in the online survey resale and user support sector, SurveyShack is the proud UK-based certified reseller of SurveyGizmo online survey tool user licenses. Under the terms of the reseller agreement, SurveyShack are bound to provide for UK-based sales, marketing and user support at competitive costs to the SurveyGizmo published global pricing. UK users of SurveyGizmo therefore benefit from full local, same-time-zone support by a team of online survey tool experts.

5.2 Security and Reliability

All details relating to the SurveyGizmo system security and reliability are available at:
https://help.surveygizmo.com/help/surveygizmo-security-faq

5.3 GDPR compliance

All details relating to the SurveyGizmo system GDPR compliance, are available at:
https://www.surveygizmo.com/privacy/gdpr/

5.4 EU-based data

Effective from 19th May 2019, all SurveyShack subscribers to the SurveyGizmo tool will be based on the EU instance of SurveyGizmo, thus ensuring all data is acquired, stored, managed and able to be deleted exclusively within the EU.

The only exception to this will be when for the purposes of providing advanced user support by the US-based SurveyGizmo support team, users have the option to temporarily grant access to their surveys and any associated data for the duration of the time required to investigate and resolve the issue.

5.5 User Support

All SurveyShack subscribers to SurveyGizmo benefit from UK-based email user support during normal working hours. All incoming support requests are immediately logged, acknowledged and prioritised as follows:

- *Low:* Resolution as soon as possible
- *Normal:* Resolution within 24 hrs wherever possible
- *High:* Resolution within the same 12hr day wherever possible
- *Urgent:* Resolution within 2 hrs or sooner

Local user support can be requested directly via our *support@surveyshack.com* email address.
Where it may be necessary to seek advanced support from the support team based at SurveyGizmo global HQ in Boulder Colorado, we reserve the option to either carry this out on the user's behalf (with their permission), or advise on how to do this directly via their support request option within the user account.