WHITE PAPER

Security White Paper

Data security is serious business.

surveygizmo

Version 3.1

Last Updated: May 2020

TABLE OF CONTENTS

CONFIDENTIAL

DO NOT DUPLICATE OR DISTRIBUTE WITHOUT WRITTEN PERMISSION FROM SURVEYGIZMO

This is a controlled document that can only be obtained from the SurveyGizmo portal, which requires that you provide your name and contact details.

This document is being given to you to help you understand the security environment and culture of SurveyGizmo and to answer questions that your security team might have. This document may be used in place of traditional security assessment checklists to help you with your due diligence. Possession of this document falls within SurveyGizmo's Terms of Use.

Our team strives to ensure accurate information, but because we are always evolving our security posture to match current and changing conditions, this document may not always reflect our exact architecture, and it may not be error-free.

We reserve the right to modify this information at any time.

For questions or comments, please email *Compliance@surveygizmo.com*.

1

EXECUTIVE SUMMARY

Since our inception, SurveyGizmo has focused on safeguarding our customers' information.

We do this while also delivering the most flexible survey platform on the market. Our customers—including some of the world's top brands across all industries—trust us to drive the insights to make informed decisions throughout their organizations.

They also trust us to keep their data safe. We take this role very seriously, embedding security measures into everything we do. Across our entire organization and throughout our platform, we deploy powerful tools and industry-leading controls to ensure the confidentiality, integrity, and availability of your data.

The purpose of this white paper is to give you an overview of our information security program and its components, which include the following areas:

- Infrastructure Architecture and Security (physical, application, and network security)
- Data Security
- People Security
- Information Security Policies and Procedures
- Audits, Certifications, and Compliance

We understand that the digital landscape is always evolving, and we are continuously improving our program. That's why we review and update our security and privacy policies continuously and work closely with industry leaders to find new and innovative ways to safeguard your data. You can rest assured that your data is safe with SurveyGizmo—today and in the future.

2

INTRODUCTION

ABOUT SURVEYGIZMO

Founded in 2006, SurveyGizmo provides an integrated feedback management platform for businesses of all sizes that enables them to collect and operationalize feedback. SurveyGizmo provides feedback and insights to more than 15,000 customers, including many of the Fortune 500, who trust us to drive the insights they need to make informed decisions. Our customers create more than 50,000 new surveys each week and receive more than one million responses each day.

HOW SURVEYGIZMO SAFEGUARDS YOUR DATA

While SurveyGizmo provides an incredibly easy-to-use platform allowing users to collect all types of data from all types of sources, we also provide a robust set of controls and tools to ensure your data is protected. Working with some of the world's top brands across all industries, we deploy industry-leading controls to make sure your data remains confidential, available, and secure.

We fully understand that together, we all bear responsibility for the data our customers share with us, so we go well beyond the standards that legislation demands. As a global provider of enterprise software, doing the right thing with data security and privacy is our bedrock.

SURVEYGIZMO'S SECURITY ORGANIZATION

Data security is a companywide priority, with security processes and practices being deployed across our business units and at each level of our organization. Our Executive Team is engaged in all information security and privacy policies, and our team directors and managers are responsible for compliance and security at the team level.

SurveyGizmo's information security program is guided by a dedicated team of professionals. Their expertise includes building, implementing, and maintaining robust cybersecurity frameworks with experience in DoD, DoE, higher education, and other public and private sector organizations.

SHARED SECURITY RESPONSIBILITY MODEL

The SurveyGizmo platform is hosted by Amazon Web Services (AWS), leveraging their robust infrastructure to increase the flexibility, reliability, and availability of our application. Security in the cloud is slightly different than security in on-premise data centers, because we operate under a shared security responsibility model with AWS.

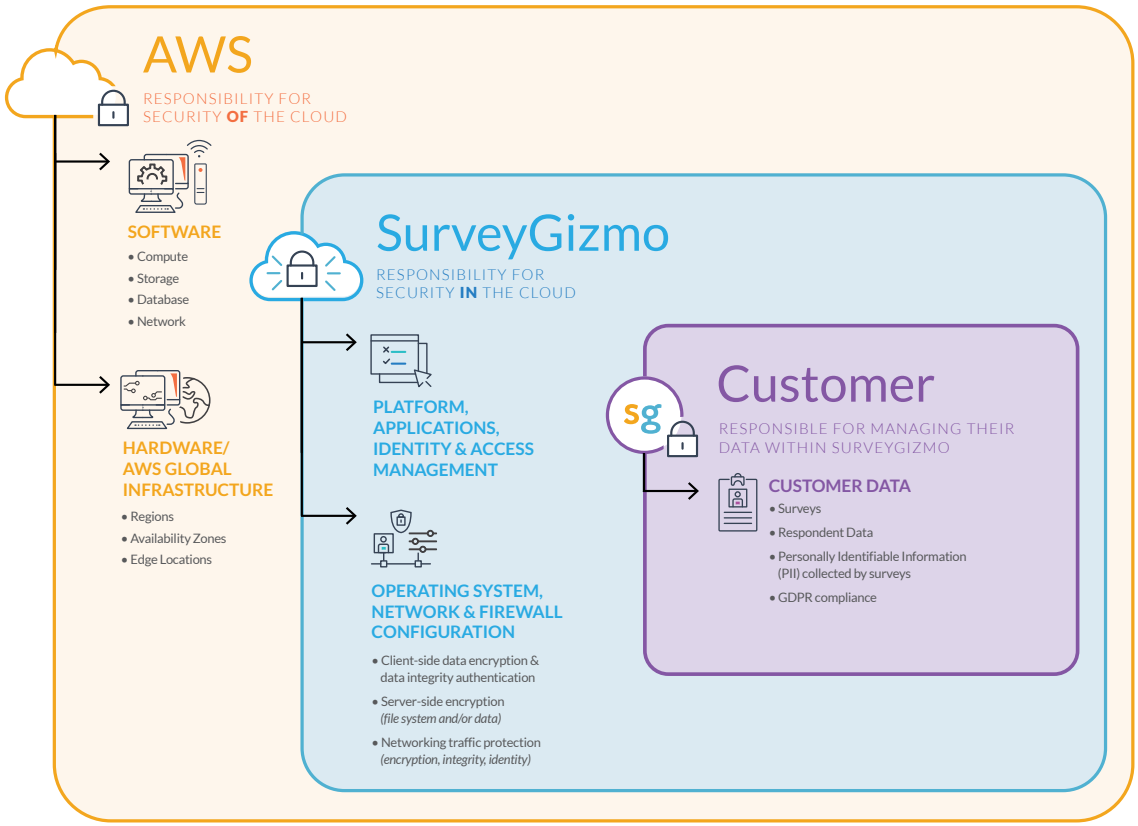
We utilize AWS for Infrastructure as a Service (IaaS), and they are responsible for the underlying infrastructure that supports the cloud. They are also responsible for protecting the global infrastructure that runs the services offered in the AWS cloud. This infrastructure includes the hardware, software, networking, and facilities that run AWS services. For more information regarding Amazon's extensive security controls, see their Overview of Security Processes Whitepaper.

SurveyGizmo is responsible for the proper configuration and logical access to the SurveyGizmo system, including the SurveyGizmo platform, applications systems, and networks.

CUSTOMER RESPONSIBILITIES

SurveyGizmo employs industry-leading best practices and gives you the tools to ensure data security, integrity, and privacy, but ultimately the security of the data you collect is in your control. That's because, as a SurveyGizmo customer, you decide what data you choose to upload into the SurveyGizmo application and where it is stored. SurveyGizmo's customer data is confidential and we do not access your data unless requested by you. This means you manage data input and verifying data output from SurveyGizmo's system.

FIGURE 1: SurveyGizmo Shared Security Responsibility Model



3

INFRASTRUCTURE ARCHITECTURE AND SECURITY

PHYSICAL SECURITY

SurveyGizmo has safeguards established to protect against physical access to customer data, including physical access controls at our corporate office, as well as the leveraged physical security that AWS provides at our data centers.

SurveyGizmo Corporate Office

SurveyGizmo's corporate office is located in Boulder, Colorado. Access to the SurveyGizmo corporate office is restricted via security badge access, and there is a strict visitor policy in place. Employees and vendors are assigned access cards based on their roles and job responsibilities, and access is revoked for all terminated employees and vendor personnel. Additionally, all visitors must be accompanied by SurveyGizmo personnel while on the premises.

Data Center Security

AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure.

Data Center Locations. SurveyGizmo operates in three of AWS's global data centers, in the United States, Canada, and Germany (European Union). In the United States, we are part of the US East (VA) Region, which has five highly redundant and reliable zones. In Canada, our data center is in Montreal, Quebec. In the European Union (EU), our data center is in Frankfurt, Germany, which is part of the EU Central region. For security reasons, and as part of the AWS policy, AWS does not provide the physical addresses of the data centers.

AWS data centers are housed in nondescript facilities. Physical access is strictly controlled, both at the perimeter and at building ingress points, by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

The data centers are sufficiently geographically separated to conform to standard disaster recovery requirements. AWS ensures that its data centers have a high level of redundancy and reliability.

Employee Access. All physical access to data centers by AWS employees is logged and audited routinely. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Security Configuration. AWS is also responsible for the security configuration of their products that are considered managed services. These services provide the scalability and flexibility of cloud-based resources with the additional benefit of being managed. For these services, AWS handles basic security tasks such as guest operating system (OS) and database patching, firewall configuration, and disaster recovery.

APPLICATION SECURITY

SurveyGizmo takes an agile approach to development that allows us to continually improve our platform and deliver the most value to our customers. To do this, we utilize a Lean Agile System Development Life Cycle (SDLC) methodology for development (see figure 2). Issues are verified, tested, and documented in Support and prioritized by the Product Development Team.

Security measures are included throughout the process. Before introduction into the production environment, our code is reviewed by quality assurance and goes through a Change Management Approval Board (CAB). Additionally, production servers are only accessed through Secure Shell (SSH) through an encrypted Virtual Private Network (VPN).

Application Environment

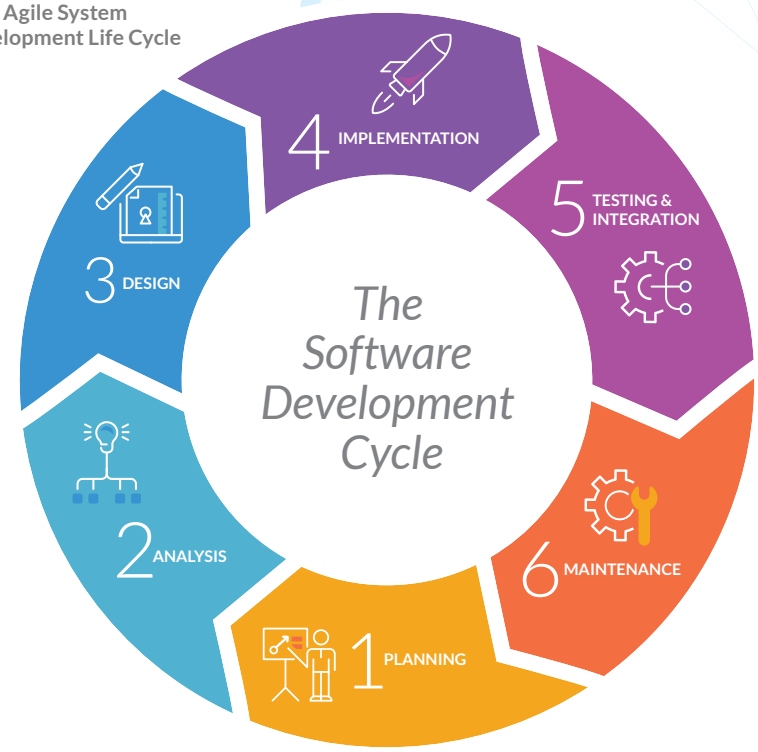
SurveyGizmo is a traditional LAMP-based application. LAMP is an acronym that stands for Linux operating system (OS), Apache HTTP Server, MySQL relational database management system (RDBMS), and PHP programming language. We've developed SurveyGizmo as a multi-tier (N-Tier) application using the Model-View-Controller (MVC) design pattern.

SurveyGizmo has separate development, test, and production environments for both our website and application. Production data is never transferred into the development or test environments.

Multi-Tier Architecture

SurveyGizmo is logically based on a three-tier client-server software architecture platform. N-Tier architecture separates user interface, application processing, and data storage function, allowing any one of the three tiers to be developed and maintained independently of the others. This creates maximum flexibility and the ability to respond to technology changes in any one tier. MVC is a software architecture pattern for implementing user interfaces on computers. These architectural decisions help to create separation of the different logical responsibilities of the application.

FIGURE 2:
Lean Agile System Development Life Cycle



100% Employee Developed

The SurveyGizmo application is currently 100% developed by employees, and all SurveyGizmo development and quality assurance activities are performed in-house. We use supported third-party libraries as necessary to enhance and produce new features.

- Source code reviews are conducted before check-in.
- Peer reviews for changes are conducted by at least two other engineers.
- We use Jenkins for automated CI/CD (continuous integration and either continuous delivery or continuous deployment) processes.
- Changes are reviewed and approved through our change approval board.

OWASP Standards

To ensure a secure application, we utilize the Open Web Application Security Project (OWASP) standards during the software development process. We focus on continually improving the functionality of our product while also improving the security of our software.

All members of Product Development are required to adhere to the OWASP top 10 standards: injection; broken authentication; sensitive data exposure; XML external entities (XXE); broken access control; security misconfiguration; cross-site scripting XSS; insecure deserialization; using components with known vulnerabilities; insufficient logging and monitoring. For more information, please see OWASP top 10.

We use a code repository along with a managed ticketing, review, and approval process. Our development team utilizes standard quality assurance procedures, and automated regression testing is performed prior to each production deployment.

Additional Security Standards

Each year, we perform a risk assessment and self-audit, and all employees receive regular security awareness training.

We do not allow unauthorized, external parties to conduct testing against our systems. It is our policy that we do not share, at any level, the policies and procedures related to the security and compliance of our systems.

NETWORK SECURITY

SurveyGizmo leverages AWS to provide a fault-tolerant, highly available, and scalable infrastructure. We employ web application firewalls and load balancers to protect against intrusion and surges in traffic volume. We are committed to providing a 99.9% uptime for survey takers and application users.

Virtual Private Cloud. We utilize a Virtual Private Cloud (VPC) and also create separate network segments using AWS Security Groups. These network segments are the equivalent of firewall rules. There are separate security groups for the different tiers of the application which restrict access on a need-to-have, least-privilege basis.

SurveyGizmo also leverages global infrastructure from AWS to better serve our customers. As a SurveyGizmo customer, you choose where your data resides, and your data remains in that data center unless you export it or request a move from our Customer Support Team.

AWS Secure Network Architecture

AWS network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACLs), and configurations to enforce the flow of information to specific information system services.

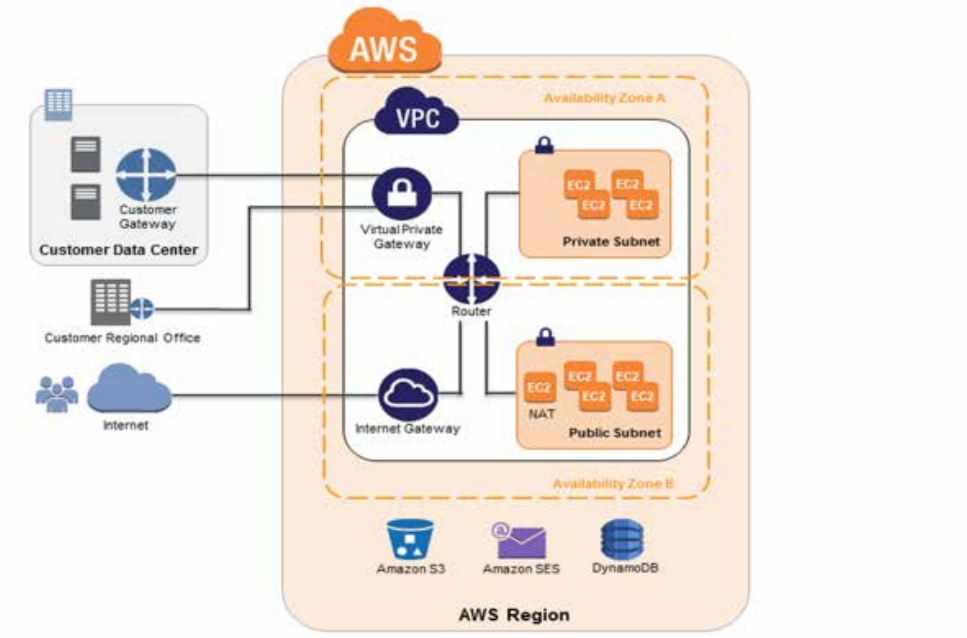
ACLs, or traffic flow policies, are established on each managed interface, which manages and enforces the flow of traffic. ACL policies are approved by Amazon Information Security. These policies are automatically pushed using AWS's ACL Manage tool to help ensure these managed interfaces enforce the most up-to-date ACLs.

AWS Secure Access Points

AWS has also strategically placed a limited number of access points to the cloud to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS). This access type allows you to establish a secure communication session with your storage or compute instances within AWS.

FIGURE 3: Amazon VPC Network Architecture

Source: Amazon Web Services: Overview of Security Processes



In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet Service Providers (ISPs). AWS employs a redundant connection to more than one communication service at each internet-facing edge of the AWS network. These connections each have dedicated network devices.

AWS Fault-Tolerant Design

Amazon's infrastructure has a high level of availability and provides its customers with the capability to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Firewalls

SurveyGizmo leverages Amazon EC2, which provides a complete firewall solution. This mandatory inbound firewall is configured in a default deny-all mode, and we explicitly open the ports needed to allow inbound traffic. The traffic is restricted by protocol, by service port, and by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block).

The AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer; thus, an instance's neighbors have no more access to that instance than any other host on the internet. They can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms. The firewall is not controlled through the guest OS; instead, it requires an X.509 certificate and key to authorize changes, adding an extra layer of security.

In order to eliminate IP Spoofing, the firewall will not permit an instance to send traffic with a source IP or MAC address other than its own.

AWS technologies:

- Web Application Firewall/CloudFront/ Route 53
  Functions Include: IDS, IPS, blacklists, DDoS and spoofing prevention
- Virtual Private Cloud/Security Groups/ Network ACLs, EC2
  Functions include: Subnet ACLs, inbound and outbound port restrictions, DMZ proxy layer

Additional technologies: The DMZ proxy layer which includes software that provides additional layer 3 – 7 protection

Host-based protection: *Functions include:* subnet/port ACLs

Backup and Reliability

All network components are configured in a redundant configuration. Customer data is stored on a primary database server with multiple active clusters for redundancy. The database servers utilize multiple data paths to ensure reliability and performance.

Automated encrypted snapshots (differentials) of databases are performed hourly, and all data storage is redundant. Encrypted daily snapshots are maintained for a minimum of 30 days, and test restores are conducted at least quarterly. Backup media resides on AWS' Simple Storage Service(S3) infrastructure, which offers global redundancy.

Data Retention

SurveyGizmo retains data that we process on behalf of our customers and data collected directly from our customers as long as it is needed to provide services. SurveyGizmo will retain and use this data as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Sometimes users have unique needs, either under specific regulations or other institutional or state requirements, that require exceptions to these guidelines. If you need your data deleted, you may contact SurveyGizmo to assist, or you can purge data within the application. Occasionally data needs to be completely destroyed after its intended use. In many cases, data is retired and locked away rather than actually destroyed (e.g., when a customer stops paying for an account, downgrades to a different account plan, etc.). This makes the loss retrievable if required. We can, however, comply with a request for total data destruction if necessary.

Because customers control their data, any subject access requests we receive from survey respondents are forwarded to the applicable customer(s), so they may take action on their data in accordance with the request.

4

DATA SECURITY

SurveyGizmo encrypts data in transit, at rest, and on all backups.

Survey data, even data designated as unencrypted, is encrypted at the disk level—"at rest." Surveys that are designated by the customer as encrypted by way of the Project Data Encryption feature are further encrypted at the row level in the database.

Additionally, customer data is backed up using Amazon Elastic Block Store (EBS) snapshots, which is used as a primary storage device for data that requires frequent and granular updates. Automated encrypted snapshots (differentials) of databases are performed hourly, and data storage is redundant.

Our redundant databases reside in a private subnet that is only accessible via our application and web servers. We also separate primary and replica databases into different AWS availability zones. In the case of a disaster, this ensures we can failover between primary and replica with minimal disruption. Additionally, we leverage Amazon's AWS security features to further lock down access to these systems.

Applications with customer-specific information are only available while employees are physically in the Boulder office or through a VPN connected to the physical office. SurveyGizmo policy does not allow employees to work from unsecured locations, like coffee shops. SurveyGizmo also has multiple employee policies, including an Acceptable Use Policy, mandatory new hire training, and quarterly security training updates.

DATA ENCRYPTION

SurveyGizmo encrypts customers' confidential data, protecting it from unauthorized access or misuse. We provide 256-bit encryption for all data at rest. This is the same level of security used by healthcare companies and the military to secure their data. All backups in our system utilize 256-bit encryption as well. Additional layers of encryption can be enabled, managed, and controlled via a client-facing feature.

Encryption Methodology and Key Strength

Encryption is accomplished using non-proprietary, industry-standard encryption algorithms. Where possible, SurveyGizmo ensures that strong encryption keys are implemented. AES-256 key length and greater are recommended encryption algorithms and key strengths.

Encryption Key Management

Encryption keys, whether created and managed by SurveyGizmo or an encryption solution vendor, are securely stored and maintained.

AWS Encryption of Data at Rest

AWS provides the ability to encrypt EBS volumes and their snapshots with AES-256. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage. In order to be able to do this efficiently and with low latency, the EBS encryption feature is only available on EC2's more powerful instance types (e.g., M3, C3, R3, G2).

User Access

Access to the SurveyGizmo application is available only through HTTPS. Data in transit is encrypted when customers choose to use HTTPS protocols for their accounts, (default), API, or survey links. We utilize TLS for our secure communication protocol, and we are currently at the most recent patch level.

Password Settings and Encryption

Passwords are stored using a salted one-way hash. Application credentials such as username/passwords are never logged. If you choose to use the login/password action, this information is stored in clear text, so this should not be used for sensitive data collection. SurveyGizmo personnel does not reset user passwords. In the event of a password being misplaced, users are sent a unique link via email, which they can use to reset their password.

SurveyGizmo is committed to helping our customers find the right balance of security and usability. To accommodate our wide range of users, our password security settings allow administrators to determine the precise level of security necessary to protect each SurveyGizmo account. *An administrator can configure these options within their account:*

- **Expiration Interval**: Set a time interval for password expiration (e.g., 3 days to 12 months)
- **Password Reuse Rules**: Disallow password reuse, either by password history or interval of time elapsed (e.g., every X password or every X months/years)
- **Minimum/Maximum Length**: Specify a minimum or maximum password length
- **Require at least one upper and one lowercase letter**: Choosing this option requires all users' passwords to contain at least one uppercase and one lowercase letter
- **Require at least one number**: Choosing this option requires all users' passwords to contain at least one number
- **Require at least one special character**: Choosing this option requires all users' passwords to contain at least one special character
- **Set up a complex rule (using Regex)**: You can specify your password pattern using Regular Expressions (Regex)
- **Password cannot contain SurveyGizmo user information**: This makes it impossible for users to incorporate their username, email address, or user ID into their password.

Survey Data Encryption

All survey data, even those that are designated as unencrypted, are encrypted at the disk level on the database servers. Surveys that are designated by the customer as encrypted are further encrypted at the row level. When surveys are flagged to be encrypted (by the customer), we further encrypt the data at the row level when it is inserted into the database on those drives.

Secure Survey Share Links

If you wish to take advantage of an extra layer of security when collecting data, you can use secure links, designated by the "https" protocol. HTTPS links use a Secure Socket Layer (SSL) to transport data safely between client and survey using an encryption algorithm.

5

PEOPLE SECURITY

Our people are an integral part of our information security program.

That's why we have developed controls throughout the employment lifecycle, allowing our employees and contractors to incorporate security measures into everyday operation.

EMPLOYEE ONBOARDING AND OFFBOARDING

Our employee security controls start before they are brought on board. We partner with an employment screening vendor to complete background checks on all employees before they are hired. Additionally, the human resources department completes reference checks on employees. We comply with the federally mandated requirements regarding I-9 (The Employment Eligibility Verification Form) documentation.

Employees are required to sign industry-standard policies including, but not limited to, Non-disclosure Agreement (NDA), Acceptable Use Policy, and Work from Home (WFH) Policy as a condition of employment.

SECURITY SKILLS ASSESSMENT AND APPROPRIATE TRAINING

Security training is a continual process. Our robust, ongoing training plan for new and existing employees ensures management support, increases employee awareness of security issues, measures our success, and allows us to improve our methods continuously. As a result, security is an integral part of our corporate culture. *Our security training initiatives include:*

- **New Hire Orientation and Training.** New employees are required to attend SurveyGizmo training, which includes security training.
- **Annual Refresher Security Awareness Training for employees.** All personnel are trained and provided with security awareness training programs at least once a year.
- **Monthly Security Trainings.** SurveyGizmo also conducts monthly security training on specific topics.
- **Monthly company meetings with the Executive Management Team.** This time is used to discuss important topics, such as security and compliance training, with the entire company.
- **Phishing Simulations and User Behavior Training.** We implemented user behavior training during which we perform benign phishing exercises on our employees. This allows us to perform ad-hoc training, identify vulnerable groups, and encourage secure email and web browsing habits.

The Vice President of Information Technology, with the support of the Director of Information Security and Compliance, is responsible for enforcing information security policies, procedures, and control techniques to address applicable requirements. Additionally, the Director of Information Security and Compliance ensures 100% participation of personnel in the Security Awareness Training Program.

Employee training is documented with their acknowledgment of completion. In addition to security training, employees understand that they are responsible for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements. They also are aware of the sanctions for non-compliance.

ENDPOINT MANAGEMENT

All employees are issued company-owned equipment, and IT administrators manage company-owned equipment. Per company policy, employees cannot access customer data from their *personal* devices, including laptops and cellphones. Employees are also aware of their responsibilities for securely leaving unattended equipment.

We use industry-standard endpoint protection software on company laptops. Laptop scanning is scheduled to run daily, and employees are encouraged to report any errors to the privileged IT Admins. We manage administrator privileges on equipment, and laptops are encrypted.

VENDOR MANAGEMENT

SurveyGizmo works with outside vendors to fulfill specific business needs and has processes in place to ensure that prospective and current vendors adhere to SurveyGizmo's security requirements and obligations.

We have developed a vendor procurement process, which includes selection criteria and assignment of vendor risk level. This process ensures that contracted vendors are adequately fulfilling the required business need. SurveyGizmo also reviews a list of vendor employees with access to SurveyGizmo systems on an annual basis, or when a use case may change.

ACCESS PROVISIONING MANAGEMENT

Access Control, Identification, and Authentication

Access to customer accounts is tightly monitored and controlled by SurveyGizmo and is provisioned to users based on the specific job on a *'need to know'* basis. Users are provided the least amount of access required to successfully complete their job requirements. A request to provision access to systems or data beyond those normally required for job responsibilities that include administrative access or elevated access to confidential data must be reviewed and approved by SurveyGizmo Senior Management. SurveyGizmo has an Acceptable Use Policy in place that provides documentation on how we may access customer data.

Individual accounts are provisioned for each employee, and depending on the system, either password or MFA is utilized to authenticate their access. Once an employee leaves, the account is terminated the same business day. Accounts are reviewed annually to ensure continued business need and validity.

Administrative Access

Administrative privileges must be limited to only those administrator accounts required to manage or maintain systems, applications, or data. Only Administrator accounts will be used to perform administrative functions. Other user accounts will have lower levels of privilege. High-level system privileges such as 'root,' administrator, SA, or default user file permissions that allow unrestricted access to computer systems are reserved for IT system administration.

Access for Third-Party IT Solution and Service Provider

SurveyGizmo utilizes AWS services to support its needs. These services include network and system infrastructure. AWS has agreed to maintain the confidentiality, integrity, and availability of the systems and data per their IT Security Policies, and contractual obligations to SurveyGizmo.

- A contract was entered into with AWS in July 2014. The standard terms of use were utilized with no customization.
- A Business Associate Agreement (BAA) was signed with AWS on June 10, 2015.
- A Data Processing Agreement (DPA) was signed with AWS on September 20, 2016.

SurveyGizmo also utilizes Salesforce for customer support ticketing.

- A contract was entered with Salesforce in 2016. The standard terms of use were utilized with no customization.
- A Data Processing Agreement (DPA) was signed with Salesforce on December 14, 2016.
- A Business Associate Agreement (BAA) was signed with Salesforce on January 23, 2017.

6

SECURITY POLICIES AND CONTROLS

BUSINESS CONTINUITY MANAGEMENT & OPERATIONAL RESILIENCE

To anticipate and prepare for possible disasters and contingencies, SurveyGizmo deploys a comprehensive set of controls to provide for the continuation of critical missions and business functions in the event of disruptions. SurveyGizmo has both a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP).

Business Continuity Plan

The SurveyGizmo Business Continuity Plan (BCP) outlines strategies that plan for both interruptions in service and continuation after a disaster. Our BCP includes the following phases: activation and notification, recovery, reconstitution, and lessons learned.

This planning ensures critical business products and services can continue to be delivered, and our employees are trained on the Business Continuity Plan each year.

The BCP identifies the types of incidents that could lead to the activation of the plan, and it includes the roles and responsibilities of SurveyGizmo staff should the plan be activated.

To help with the ranking of tasks, the BCP includes a Business Impact Analysis (BIA), which was developed by determining the business processes and recovery criticality, identifying resource requirements, and then identifying recovery priorities for system resources.

The BCP also identifies the critical business functions needed to ensure the availability of essential services and programs and ensures the continuity of operations. Continuity planning is one component of a much broader emergency preparedness process and includes items such as contingency planning, business practices, and operational continuity.

As one component of our comprehensive risk management approach, our BCP identifies potential vulnerabilities and threats and then implements approaches to either prevent such events from happening or limit their potential impact.

Disaster Recovery Plan

Disasters cannot be prevented, but steps can be taken to eliminate or reduce the impact of the disaster on the business. A great deal of consideration is taken to ensure that if a disaster occurs, the necessary strategies are in place to reduce the impact on our customers. The SurveyGizmo Disaster Recovery Plan (DRP) outlines how to recover information technology and information systems in the event of a disaster.

SurveyGizmo has a DRP that includes shared responsibilities with Amazon, and it is reviewed annually. Amazon utilizes disaster recovery facilities that are geographically remote from its primary data center. When using the AWS disaster recovery shared security model, they provide the physical infrastructure, network, and operating systems, and SurveyGizmo ensures the proper configuration and logical access to the resources.

Some of the preventive measures that SurveyGizmo utilizes include ensuring proper support for data migration and durable storage from AWS, ensuring proper alerting, ensuring good backups, ensuring employees have connections from their homes, and monitoring early warning systems.

The DRP identifies the requirements to recover the information technology assets from a disaster. It also defines the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) and Maximum Tolerable Downtime (MTD).

The following recovery plan objectives have been established for SurveyGizmo:

- Identify the activities, resources, and procedures to carry out SurveyGizmo's processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated personnel and provide guidance for recovering SurveyGizmo during prolonged periods of interruption to normal operations.
- Coordinate Disaster Recovery planning activities with Business Continuity actions and Incident Response activities.
- Ensure coordination with external points of contact and vendors associated with SurveyGizmo.
- Ensure coordination with other plans associated with SurveyGizmo.

Plan Testing

SurveyGizmo conducts annual tests of the BCP and DRP. Tests and exercise events measure plan effectiveness, ensuring that all personnel know their roles and are informed of the specific actions required of them. The test results are documented, and actions are taken so that the associated plans, policies, and procedures can be updated.

Service Health and Failover

Customers can subscribe to the SurveyGizmo Status IO page for notification of issues related to the SurveyGizmo application. https://surveygizmo.statuspage.io/

As the SurveyGizmo application is completely reliant on the availability of AWS, customers can customize the following AWS page for their availability. http://status.aws.amazon.com/

Also, if you send emails via the SurveyGizmo application, you can ensure that RackSpace (the hosting provider for email service) is available via the following page. https://rackspace.service-now.com/system_status/

We currently do not allow our customers to move away from either AWS or RackSpace as the hosting provider.

CHANGE CONTROL & CONFIGURATION MANAGEMENT

Because system modifications can introduce risks to system integrity or reliability, as well as threats to data confidentiality, SurveyGizmo has a comprehensive change management plan in place. This includes the controls needed to manage system modifications while identifying threats to data confidentiality and maintaining system integrity and reliability.

The change management process includes requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. It begins with the creation of a change request within SurveyGizmo's selected technology platform and ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties.

The system risk impact from changes and the risk probability of adverse events fall into three categories:

- **Low**: If an adverse event is encountered, the financial damage or confidential data exposure is minimal or non-existent. The risk of an adverse event is statistically very low. It would require prevention measures that outweigh the expenditure of resources (time or money) to gain a significant improvement in order not to encounter this risk.
- **Medium**: If an adverse event is encountered, the financial damage or confidential data exposure impact is moderate and could be outside of the risk tolerance for SurveyGizmo. The risk of an adverse event is statistically moderate, and the investment of resources to mitigate the possibility of an event would essentially cost about as much as the impact of the event in resources.
- **High**: If an adverse event is encountered, the financial damage could be high, and the exposure of confidential data could be widespread or critical. The risk of an adverse event is statistically high. The adverse effects far outweigh the investment in resources to significantly reduce the likelihood of an event or to reduce the overall risk impact of damages to place it into a lower Risk Impact category.

In addition to impact and probability, the scope or number of components touched during a change also can partially determine the security risk. In general, more places touched means the potential for more risk. SurveyGizmo defines scope as small, medium, large, and extra-large, with extra-large being the riskiest.

THREAT AND VULNERABILITY MANAGEMENT

At SurveyGizmo, we identify, evaluate, treat, and patch network and application vulnerabilities through continual vulnerability management efforts. Your data is protected with numerous anti-hacking measures, redundant firewalls, and constant security scans. This decreases the risk as well as the exposure time during which vulnerabilities can be exploited.

Penetration Testing

SurveyGizmo performs regular penetration testing of the application and infrastructure. We employ a reputable third party to perform annual penetration testing. SurveyGizmo works to resolve identified issues, then conducts follow-up third-party testing to ensure vulnerabilities are adequately addressed.

Continual Security Scans

SurveyGizmo utilizes a reputable third-party tool to perform continuous scans of our application as well as weekly scans of our network.

Intrusion Detection and Prevention

To help identify threats, cyber-attacks, or other security events, SurveyGizmo utilizes intrusion detection (IDS) at multiple layers of the application, with extensive logging and alerting capabilities. We monitor criteria for thousands of different alerts ranging from customer experience and application health to server and service metrics.

Logs and Alerts. Firewall logs and other access logs (e.g., HTTP) are restricted to authorized users via secure multi-factor authentication (MFA) controls. We utilize Amazon's Recommended MFA, and only our privileged IT Admins have access to this information.

Log Access and Storage. Logs are kept for a minimum of 90 days and are stored in AWS. We maintain user access log entries that contain the date, time, customer information, operation performed, and source IP address. If there is suspicious or inappropriate use, SurveyGizmo can provide customer log entry records to assist in analysis.

Robust monitoring software is used to monitor performance and notify us of any problems in our production environment. The checks include, but are not limited to, business logic, database layer, disk space, resources, and application logs.

Logically Separated Data.

In order to ensure that data collected for different purposes can be processed separately, SurveyGizmo logically separates the data of each of its clients. Each customer has a unique username (email address) and a unique password, and data segmentation is keyed off unique customer IDs. We're also able to scale horizontally to support increasing users and customers.

Brute Force Attack Protection

After repeated unsuccessful logins, the lockout features prevent the login page from being resubmitted.

Background Queued Processes

We leverage a number of queuing systems to defer jobs that do not need to be transactional. This allows us to scale up and down the number of queues and workers to mirror the demands on our systems without impacting the front-end experience of users in the application.

Redundant Data Store

To ensure that we never lose any of our customers' data, we have multiple strategies utilizing redundant data stores. These include master/read databases and in-memory caching.

INCIDENT RESPONSE MANAGEMENT

The ability to respond to incidents is a significant aspect of any information technology program. Preventive activities such as application scanning, password management, intrusion detection, intrusion prevention systems, firewalls, risk assessments, malware and antivirus prevention, and user awareness and training can reduce the number of incidents. However, not all incidents can be prevented.

SurveyGizmo has implemented an Incident Response Plan (IRP) that covers Incident Response Requirements (IRRs), roles and responsibilities of each Incident Response Team member, Incident Reporting Procedures, Incident Handling Procedures, and complementary metrics. SurveyGizmo employees are trained in the procedures, including how and when to escalate an issue. We have procedures for normal business hours as well as for after-hours and weekends.

Breach Notification

Suspected incidents are reported to the Team Managers, who are responsible for organizing the investigation and notifying internal stakeholders. If the investigation finds a need for containment, that will occur, and then analysis will follow. If repair, recovery, or remediation is needed, that will follow.

Notifications to clients will be made based on contractual or legal obligations, reporting will be made to Executive Management, and training issues will be addressed. If a breach is detected with your data, you will be notified as soon as we are able.

Patching

Production servers are frequently patched to ensure their security is always up to date. We roll patches out through the development rollout process—from development to Quality Assurance (QA) to production. We mitigate vulnerabilities within our predefined timeframes.

Local systems are protected with industry-standard antivirus software. Production servers are Linux-based and frequently patched to ensure their security is always up to date. In correlation with our Agile sprint schedules, security patches are applied within two sprints of notification of the patches being available.

When vulnerabilities are identified, our mitigation scale is as follows:

- **Critical:** addressed immediately (within 4 hours)
- **High:** addressed within 3 days
- **Medium:** included in the next appropriate sprint

Governance & Risk Management

The SurveyGizmo Information Security and Risk Management Program integrates risk identification and mitigation with policy and regulatory information security compliance management. This program leverages industry best practices, guidelines, and standards and includes the following elements.

SurveyGizmo will:

- Perform an Information Security Risk Assessment and analysis at least once per year.
- Develop and implement policies and standards to meet information security risk mitigation objectives as well as maintain compliance with privacy and other regulatory requirements.
- Establish a remediation prioritization process that allocates a priority level to the threat and vulnerabilities with the potential to cause significant impact or harm to SurveyGizmo services, systems, devices, or confidential data.
- Perform an information security risk assessment and select adequate controls to mitigate known risks. The controls will be consolidated in a Risk Register. An Information Security Risk Assessment will be performed prior to the deployment of new or modified systems.

Risk Determination is used to assess the level of risk to the IT systems. The determination of risk for a particular threat or vulnerability pair will be measured using a risk level matrix. The risk level matrix will be expressed in terms of probability and impact level, as shown below:

FIGURE 4: Risk-Level Matrix

LIKELIHOOD \ IMPACT	10	20	30	40	50	60	70	80	90	100
0.1	1	2	3	4	5	6	7	8	9	10
0.2	2	4	6	8	10	12	14	16	18	20
0.3	3	6	9	12	15	18	21	24	27	30
0.4	4	8	12	16	20	24	28	32	36	40
0.5	5	10	15	20	25	30	35	40	45	50
0.6	6	12	18	24	30	36	42	48	54	60
0.7	7	14	21	28	35	42	49	56	63	70
0.8	8	16	24	32	40	48	56	64	72	80
0.9	9	18	27	36	45	54	63	72	81	90
1	10	20	30	40	50	60	70	80	90	100

LOW | MED | HIGH

7

AUDITS, CERTIFICATIONS, AND COMPLIANCE

SurveyGizmo's information security program is built on industry best practices.

Audits, certifications, and compliance ensure we are adhering to established policies, standards, and procedures. This also allows us to address any nonconformities, so we remain in compliance.

- SurveyGizmo participated in a SOC2 Type I audit in 2019 with the purpose of assuring our customers we have a mature, continuous monitoring program. Our SOC2 Type II scoping period will cover security and availability for 2020 – 2021 and every year thereafter.
- We have engaged with a third-party auditor to begin our ISO 270001 series certification, expected end of year in 2020.
- We are also in compliance with PCI DSS standards to maintain a secure environment to process, store, or transmit credit card information.

SurveyGizmo is proud to comply with these standards and certifications, using them as a foundation upon which we can continually hone our information security practice.

REFERENCES

This document was created with the following references:

https://aws.amazon.com/compliance/resources/

https://aws.amazon.com/security/

https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf