Quipu®

Library focused. Library approved.

Information Security Policy

CONTENTS

Company Information

The Quipu Group, LLC (Quipu) provides consulting, web application development and web application services primarily to the library industry. Quipu currently is operated solely by its owners and therefore believes that an ISO or NIST security policy framework does not accurately fit our situation and size.

Therefore, Quipu has developed this Written Information Security Policy based on our existing policies and best practices from ISO, NIST, SANS, Commonwealth of Massachusetts 201 CMR 17.00 Compliance Checklist and other sources. Two of the primary owners of Quipu maintain, control, and access the hosted servers used to provide our services.

Quipu, since inception in 2005, has not had a breach of data owned or maintained by Quipu.

Purpose

The purpose of the Information Security Policy is to:

a. Ensure the security, confidentiality, integrity, and availability of personal and other sensitive information Quipu collects, creates, uses, and maintains.
b. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.
c. Protect against unauthorized access to or use of Quipu-maintained personal and other sensitive information that could result in substantial harm or inconvenience to any client or client's end-users.
d. Define an information security program that is appropriate to Quipu's size, scope, and business; its available resources; and the amount of personal and other sensitive information that Quipu owns or maintains on behalf of others, while recognizing the need to protect both customer and end-user information.
e. Formalize response procedures for Disaster Recovery and Data Breaches.

Scope

This Information Security Policy applies to all owners, employees, contractors, officers and directors of Quipu. It applies to any records that contain personal and other sensitive information in any format and on any media, whether in electronic or paper form.

General Information Security

1. Information Security Manager

   Quipu has designated owner Scott Stockton to be the Information Security Manager. Duties include all network and server security including, but not limited to, assigning user access to all servers (hosted or local) maintained or accessed by Quipu.

2. Password Policy

   Quipu's password policy consists of strong password creation and storage. Passwords created by Quipu shall be:

   a. At minimum, a 14-character password including digits and symbols Or
   b. Pass Phrase

   Storage of passwords shall be in an approved storage application that employs encryption and username/password entry.

3. Server Security

   a. Hosted Servers

      Quipu contracts with Linode.com for our servers and Linode contracts with data centers. Linode and data centers provide for physical security to the data centers. Servers in use employ network firewalls and Quipu additionally institutes local firewalls.

      Quipu addresses malware, viruses, etc. by:
      i. Email servers for our web applications allow only sending from our web applications. Email servers do not accept incoming email. Email servers also don't relay emails.

      ii. Our servers are setup so that any interaction is through our web applications. Therefore malware, etc. cannot be downloaded/executed on our servers.

   b. Remote Access

      Quipu utilizes hosted servers for its services. Access to these servers is controlled with username/password authentication and all allowable users and user access levels are determined/maintained by the Information Security Manager.

   c. Server Access

      Quipu limits access to servers to the owners and selected contractors. Quipu employs user level access restrictions for contractors.

4. Safeguards
    a. Quipu will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal or other sensitive information that Quipu owns or maintains on behalf of others.

    b. Safeguards shall be appropriate to Quipu's size, scope, and business; its available resources; and the amount of personal and other sensitive information that Quipu owns or maintains on behalf of others, while recognizing the need to protect both client and client's end-users' information.

    c. Quipu's administrative safeguards shall include, at a minimum:
        1. Designating one or more employees to coordinate the information security program.
        2. Identifying reasonably foreseeable internal and external risks and assessing whether existing safeguards adequately control the identified risks.
        3. Selecting service providers that are capable of maintaining appropriate safeguards and requiring service providers to maintain safeguards.
        4. Adjusting the information security program in light of business changes or new circumstances.
        5. Continuation of technology specific insurance to cover identity theft or disclosure of nonpublic personal information.

    d. Quipu's technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:
        1. Secure user authentication protocols, including:

            i. Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;

            ii. Restricting access to active users and active user accounts only, including preventing terminated employees or contractors from accessing systems or records; and

iii. Blocking access to a user identifier after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

2. Secure access control measures, including:

   i. Restricting access to records and files containing personal or other sensitive information to those with a need to know to perform their duties; and

   ii. Assigning unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) to each individual with computer or network access that are reasonably designed to maintain security.

3. Encryption of all personal [or other sensitive] information traveling wirelessly or across public networks.
4. Encryption of all personal or other sensitive information stored on laptops or other portable or mobile devices, and to the extent technically feasible, personal, or other sensitive information stored on any other device or media (data-at-rest).
5. Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal or other sensitive information or other attacks or system failures.
6. Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal or other sensitive information.
7. Reasonably current system security software (or a version that can still be supported with reasonably current patches and malware definitions) that

   i. includes malicious software ("malware") protection with reasonably current patches and malware definitions, and

   ii. is configured to receive updates on a regular basis.

e. Quipu's physical safeguards shall, at a minimum, provide for:

   1. Defining and implementing reasonable physical security measures to protect areas where personal or other sensitive information may be accessed, including reasonably restricting physical access and storing records containing personal or other sensitive information in locked facilities, areas, or containers.

2. Preventing, detecting, and responding to intrusions or unauthorized access to personal or other sensitive information, including during or after data collection, transportation, or disposal.

3. Secure disposal or destruction of personal or other sensitive information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

Web Application Policies

1. Purpose
   The purpose of the Web Application Policy is to:
   a. Ensure the security, confidentiality, integrity, and availability of personal and other sensitive information Quipu collects, creates, uses, and maintains for use in a client specific, web application.
   b. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.
   c. Protect against unauthorized access to or use of Quipu-maintained personal and other sensitive information that could result in substantial harm or inconvenience to any client or client's end-users.
   d. Define a Web Application Security program that is appropriate to Quipu's size, scope, and business; its available resources; and the amount of personal and other sensitive information that Quipu owns or maintains on behalf of others, while recognizing the need to protect both client and client's end-users' information.

2. Scope
   This Web Application Policy applies to all web applications developed, maintained and hosted by Quipu.

3. Information Transmission
   All interactions with Quipu's web applications shall be via SSL/TLS or other reasonable technology, unless otherwise specified by client.

4. Information Storage, Use and Disposal
   Storage – All Personally Identifiable Information (PII) collected by Quipu for performance of the web-application service and all client system connection information shall be stored using Advanced Encryption Standard (AES) 128-bit key length at a minimum.

   Encryption keys used to encrypt said data shall not be stored within the same database as the encrypted data.

Use – Use of PII and client's system information shall be used solely for the web-applications purpose and shall not be disclosed.

Disposal – If client wishes to discontinue use of the web application, all data shall be sent to the client (upon request) and then removed from Quipu's hosted servers.

5. Personally, Identifiable Information (PII)
   Quipu considers PII to include any nonpublic information that on its own or in conjunction with other information, can identify, contact or locate a single person.

   Quipu’s web applications will minimize as much as possible the collection of PII while still providing the necessary service.

   Quipu’s web applications will employ Advanced Encryption Standard (AES) 128-bit key length at a minimum. Encryption keys used to encrypt said data shall not be stored within the same database as the encrypted data.

   The following information, if collected, will be encrypted and includes but is not limited to:
   a. Social Security Number
   b. Driver’s license number and other government issued identification numbers.
   c. Financial data such as credit/debit card numbers, with or without any required security code, access code, personal identification number or password that would permit access to the individual’s financial account.
   d. Any personally identifiable financial information or consumer list, description or other grouping derived from personally identifiable financial information, where personally identifiable financial information includes any information provided by a consumer in the course of using a web-application controlled/designed by Quipu.
   e. Health Information
   f. Contact information such as email, phone and mail addresses.

   Transmission of PII information within Quipu’s web applications will occur using encrypted secure communication such as HTTP over SSL/TLS or other such encryption protocols as developed and adopted.

6. DDOS (Distributed Denial of Service) Attacks
   In addition to standard network protection maintained by linode.com, Quipu additionally uses fail2ban to protect against SSH attacks.

7. SQL Injection
   Quipu employs coding techniques to thwart SQL Injection including but not limited to:
   a. Parameterized queries
   b. Examination and untainting of all data entered by user

Data Breach Procedures

1 Purpose
The purpose of the Data Breach Procedures is to:
   a. Layout the steps to be performed by Quipu in the event of a Data Breach.
   b. Define who is to be notified in case of a data breach.
   c. Define actions to re-secure access to the protected data.
   d. Define actions to be taken to remedy issues related to such a breach.

2 Scope
This Data Breach Procedure applies to all data maintained by Quipu on its hosted servers, internal servers and computers.

3 Notification
In the event of a Data Breach, Quipu will notify the following:
a. Attorney General of Colorado
b. All Clients affected by the data breach
c. Quipu’s insurance provider

4 Restore Security
Quipu will block all access to the information until at such time enhanced security measures are put in place. Once in place, where applicable, Quipu will restore access to client and client's end users.

5 Review
After a Data Breach and once restoration procedures have been accomplished, Quipu will review the Data Breach incident to further enhance security.

Disaster Recovery Procedures & Policy

1 Purpose
The Disaster Recovery Procedures define actions to be taken by Quipu in order to restore service to web applications developed, maintained and hosted by Quipu.

2 Scope
The Disaster Recovery Procedures apply to all owners, employees, contractors, officers and directors of Quipu. Disaster recovery occurs when a service hosted and maintained by Quipu becomes unavailable due to physical or virtual problems.

3 Software & Database Backups
Local backups of software/web-applications and databases are performed nightly and stored for 7 days. These backups are rotated every 7 days.

Remote System backups are performed nightly and stored for 7 days and rotated every 7 days.

4 System Backup
Quipu maintains system level backups nightly and are stored for 7 days. These backups are rotated on a 7-day schedule.

In addition, a weekly system backup is performed and stored for 2 weeks. These backups are rotated on a 2-week basis.

5 Physical Disaster
In the event there is a physical disaster to a data center, Quipu will work with Linode/Hosting Provider in order to restore service.

Testing and Compliance

Once yearly and more frequently when warranted, the owners of Quipu review the above security policies and make any changes necessary to code and data storage deemed necessary.