Better Ways Accounting & Tax PRIVACY STATEMENT

Last Updated January 1, 2022

Better Ways Accounting & Tax (“us,” “we,” or “our”) thank you for visiting the online and mobile resources we publish. We use the words “you” and “your” to mean you, the reader, and other visitors to our online and mobile resources who are, in all cases, over the age of 13. Our privacy statement (“this statement,” “this privacy statement,” and “our statement”) informs you about from whom and the types of personal information we collect, how we use it, who we share it with and why, and what we do to try to protect it.

Online and mobile resources mean the websites and other internet features we own that allow you to interact with our websites, as well apps we’ve created and distributed to let our customers and followers view our online and mobile resources or otherwise interact with the content we provide.

WHO WE COLLECT PERSONAL INFORMATION FROM

We may collect personal information from the following groups of data subjects: visitors to, and users of, our online and mobile resources; our customers; current members of our workforce and those who apply for posted jobs; and third-party vendors and business partners.

Personal information generally means information that can be used to identify you or that can be easily linked to you (for example, your name, address, telephone number, email address, social security number and date of birth). The privacy laws in some jurisdictions include unique elements in what they consider to be the personal information of the consumers or data subjects they protect. If those laws apply to us, as in the case of the California Consumer Privacy Act (“CCPA”) or European General Data Protection Regulation (“GDPR”), our use of the phrase “personal information” includes the unique elements required by such laws.

The categories of information we collect from each of these groups, and the ways in which we use it, differs. As you may have noticed, it’s possible that the same person could fall into more than one group. Most of this statement addresses our processing and sharing of personal

information collected from visitors to and users of our online and mobile resources and our customers.

Nonetheless, we collect and retain the types of professional or employment-related personal information you would expect an employer to have about its existing and former workforce and new job applicants. We provide legally required notices of collection and describe our use and sharing of the personal information of our workforce and applicants in greater detail in confidential internal human resource manuals and documents accessible to members of our workforce, or by publication on the proprietary workforce/applicant portals and apps we operate. In some cases, such portals and apps may be operated by third parties who transfer the personal information to us. In those situations, the legal responsibility to provide notice usually rests with the third party, not us.

In addition, like all corporate enterprises, we buy goods and services, lease equipment and office space and attend industry events. In doing so, we interact with many existing and potential vendors and business partners from whom we necessarily collect certain personal information in connection with our contractual and business relationships. As with our customers, this information is typically limited to minimum business contact information. We use and share personal information collected from our vendors and business partners to manage, administer and perform under our contracts with them, or share information about our products. We describe our use of vendor and business partner personal information in greater detail in our confidential contracts with those parties or on the internal vendor management portals we operate.

WHAT WE COLLECT

There are two types of information that we obtain from you online and then store and use: (i) non-personal information that's collected automatically from each visitor, such as your device operating system; and (ii) personal information that you voluntarily provide to us or that is collected automatically.

By using our online and mobile resources or purchasing our products or services, you are signifying to us that you agree with this section of our privacy statement and that we may use and disclose your information as described.

Voluntarily Submitted Information.

If you participate in certain activities via our online and mobile resources, you may be asked to provide us with information about yourself. The types of personal information we collect in those situations includes identifiers (such as your name, email address, physical address, and phone number), professional information (such as the business you are in), and financial account information (such as your credit card information). We do not sell, rent, or trade voluntarily submitted personal information with third parties.

If you don't want us to collect this type of personal information, please don't provide it. This means you shouldn't participate in the activities on our online and mobile resources that request or require it and you may want to communicate with us by phone or regular mail instead. Participation is strictly your choice. Not participating may limit your ability to take full advantage of the online and mobile resources, but it will not affect your ability to access certain information available to the general public on the online and mobile resources.

Some of the ways you voluntarily give us your personal information and how we use it:

Emails and Online Forms – When you send us an email or fill out an online form, such as to contact us, your email address and any other personal information (e.g., home address or phone number) that may be in the content of your message or attached to it, are retained by us and used to respond back directly to you and to process your request. Depending on the personal information provided, communications from us may be in the form of emails, telephone calls, and/or text messages. We may also send you information about any of our products or services we think may be of interest to you.

Registering for an Account – When you register for an account or you register your child for a sub-account, you submit personal information to us such as your name and email address (or your child's name and email address) which we then retain. We use that information to create and manage your account and, in some cases, establish a password and profile to communicate with you and any sub-accounts you created via email.

Registering for Events – When you register for services, webinars, events, conferences, or programs we ourselves may host (rather than

outsource to a third-party event manager with its own privacy policies), you will be submitting the types of identifiers described above. If the event requires a fee, we may also ask you to submit credit card or other financial information. We use this information to register you for the event and send you communications regarding the event.

Becoming a Subscriber to Our Service – We use any information provided from our customers to perform our contractual obligations and provide the products and services purchased to them, to manage their accounts and communicate with them.

Social Media and Community Features – Some of our online and mobile resources may offer social media-like community features letting users post messages and comments, and/or upload an image or other files and materials. If you choose to make use of these features, the information you post, including your screen name and any other personal information, will be in the public domain and not covered/protected by this statement.

Automatically Collected Information.

When you visit our online and mobile resources, basic information is passively collected through your web browser via use of tracking technologies, such as a “cookie” which is a small text file that is downloaded onto your computer or mobile device when you access the online and mobile resources. It allows us to recognize your computer or mobile device and store some information about your preferences or past actions.

We allow third party vendors to use cookies or similar technologies to collect information about your browsing activities over time following your use of the site. For example, we use Google Analytics, a web analytics service provided by Google, Inc. (“Google“). Google Analytics uses cookies to help us analyze how you use the online and mobile resources and enhance your experience when you visit the online and mobile resources. For more information on how Google uses this data, go to www.google.com/policies/privacy/partners/. You can learn more about how to opt out of Google Analytics by going to https://tools.google.com/dlpage/gaoptout.

The internet activity information collected through cookies and other similar means includes such things as: the domain name and IP address from which you accessed our online and mobile resources; the

type of browser and operating system you use; the date and time and length of your visit; the specific page visited, graphics viewed and any documents downloaded; the specific links to other sites you accessed from our online and mobile resources; and the specific links from other sites you used to access our online and mobile resources.

Additionally, if you access our online and mobile resources from a phone or other mobile device, the mobile services provider may transmit to us uniquely identifiable mobile device information which allows us to then collect mobile phone numbers and associate them with the mobile device identification information. Some mobile phone vendors also operate systems that pinpoint the physical location of devices and we may receive this information as well if location services are enabled on your device. If you do not want us to collect and use geolocation data, disable location services through your device settings.

Regardless, we use both automatically collected information and mobile device information to compile generic reports about popular pages on our online and mobile resources and to see how our customers and followers are accessing our online and mobile resources. We then use that

data to administer the online and mobile resources and make them better, make your activities more convenient and efficient and to enhance the functionality of our online and mobile resources, such as by remembering certain of your information in order to save you time.

We use and retain your personal information in accordance with applicable law and as long as necessary to carry out the purposes described above in accordance with our internal data retention procedures.

User Beware: External Sites, Apps, Links and Social Media.

We maintain a presence on one or more external social media platforms such as Twitter, Facebook, YouTube and LinkedIn. We may further allow features of our online and mobile resources to connect with, or be viewable from, that external social media presence. Similarly, our online and mobile resources may contain links to other websites or apps controlled by third parties.

We are not responsible for either the content on, or the privacy practices of, social media platforms, or any third-party sites or apps to

which we link. Those apps, sites and platforms are not controlled by us and therefore have their own privacy policies and terms of use. If you have questions about how those apps, sites and platforms collect and use personal information, you should carefully read their privacy policies and contact them using the information they provide.

WHEN/WITH WHOM DO WE SHARE PERSONAL INFORMATION

We use non-personal information to administer our online and mobile resources, make them better, and to make business decisions about what programs our customers might like.

We use voluntarily provided personal information to respond to your inquiries and provide you with the services you have requested, amongst other uses as further described below. We do not sell or rent your personal information to third party data vendors or marketing companies. As you might expect, we disclose your information when required by law.

Affiliates.

In addition to those third parties set forth above, we may share your information, including personal information, within our family of companies. Those companies will use such information in generally the same manner as we do under this privacy statement which includes sending you information about their products, services, or initiatives that may be of interest to you.

Legally Compelled Disclosures.

We may disclose your information, including personal information, to government authorities, and to other third parties when compelled to do so by such government authorities, or at our discretion or otherwise as required or permitted by law, including but not limited to responding to court orders and subpoenas.

To Prevent Harm.

We may disclose your information, including personal information, when we have reason to believe that someone is causing injury to or interference with our rights or property, other users of the online and mobile resources, or anyone else that could be harmed by such activities.

Business Transfer.

If we or any of our affiliates, or substantially all of its or their assets, are acquired by one or more third parties as a result of an acquisition, merger, sale, reorganization, consolidation, or liquidation, personal information may be one of the transferred assets.

Vendors and Business Partners.

We may share your information, including personal information, with our vendors and other third parties with whom we have a contractual relationship. We may also share your information, including personal information, with vendors who provide third party software services that you have chosen to assist you with your sales funnels. We do our best to disclose only the information each of those parties need.

We have adopted standards for those vendors and business partners who receive personal information from us. We attempt to bind such vendors and business partners to those standards via written contracts. We further attempt to contractually restrict what our vendors and business partners can do with the personal information we provide to them such that it is used only to the extent necessary to carry out the business purpose for which it was provided; is not disclosed to anyone else without our consent or under our instruction; remains, as between us and the applicable vendor or business partner, our property; and is not transferred out of the United States without our consent.

Please note, however, that we cannot guarantee that all of our vendors and business partners will agree to these contractual requirements; nor can we ensure that, even when they do agree, they will always fully comply.

YOUR RIGHTS AND OPTIONS

You do not have to provide personal information to enjoy most of the features of our online and mobile resources. Moreover, you can opt-out of certain activities like newsletters and announcements. Residents of California and data subjects whose personal information was obtained while they were in the GDPR Jurisdictions have certain additional rights.

GDPR Jurisdictions means the countries composed of the European Economic Area (including Iceland, Lichtenstein, and Norway) and the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech

Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

Furthermore, Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and Japan have received an "adequacy decision" from the European Commission, adheres to the material terms of the GDPR. Switzerland also has its own data protection via its Federal Act of Data Protection ("DPA").

GDPR longer has jurisdiction over The United Kingdom. Since the United Kingdom ("UK") has now formally left the European Union, it is no longer regulated domestically by the material terms of the GDPR. The United Kingdom General Data Protection Regulation ("UK-GDPR") is the UK's data privacy law that governs the processing of personal data domestically.

If we are using personal information you provided to us in order to enable us to send you materials, such as newsletters or product alerts via text or email, and you decide you don't want to receive such materials, you may opt-out by following the opt-out instructions in the email or other communication (e.g., by responding to the text with "STOP"), or by contacting us using the contact information below. When we receive your request, we will take reasonable steps to remove your name from our distribution lists. You need to understand it may take a period to remove your name from our lists after your request and due to such latency, you may still receive materials for a period of time after you opt-out. In addition to opting out, you have the ability to access, amend, and delete your personal information by contacting us using the contact information below.

Some browsers have a "do not track" feature that lets you tell websites that you do not want to have your online activities tracked. At this time, we do not specifically respond to browser "do not track" signals.

CHILDREN'S PRIVACY

Federal law imposes special restrictions and obligations on commercial website operators who direct their operations toward and collect and use information from, children under the age of 13. We take those age-related requirements very seriously, and consistent with it do not intend

for our online and mobile resources to be used by children under the age of 13 without first obtaining the verifiable consent of such child's parent or legal guardian. Moreover, we do not knowingly collect personal information from minors under the age of 13, only a parent or legal guardian may provide such information after adhering to our verification process for submitting such information via the online and mobile resources. If we become aware that anyone under the age of 18 has submitted personal information to our online and mobile resources, we will delete that information and will not use it for any purpose whatsoever. If you believe that someone under the age of 18 has submitted personal information to our online and mobile resources, please contact us at john@betterwaysaccounting.com. We encourage parents and legal guardians to talk with their children about the potential risks of providing personal information over the Internet.

HOW WE PROTECT COLLECTED PERSONAL INFORMATION

We will take all reasonable security precautions to protect your personal information provided to our online and mobile resources. We have adopted a security program that includes technical, organizational, administrative, and other security measures designed to protect, in a manner consistent with accepted industry standards and applicable law, against anticipated or actual threats to the security of personal information (the "Security Program"). We cannot, however, guarantee that your information, whether during transmission or while stored on our systems or otherwise in our care, will be free from unauthorized access or that loss, misuse, destruction, or alteration will not occur. Except for our duty to maintain the Security Program under applicable law, we disclaim any other liability for any such theft or loss of, unauthorized access or damage to, or interception of any data or communications including personal information. We have every reason to believe our Security Program is reasonable and appropriate for our business and the nature of foreseeable risks to the personal information we collect. We further periodically review and update our Security Program, including as required by applicable law.

Nonetheless, as part of our Security Program, we have specific incident response and management procedures that are activated whenever we become aware that your personal information was likely to have been compromised. We further require, as part of our vendor and business partner oversight procedures, that such parties notify us immediately if they have any reason to believe that an incident adversely affecting

personal information, we provided to them has occurred.

THE CALIFORNIA CONSUMER PRIVACY ACT

When we collect personal information from California residents, we become subject to, and those residents have rights under, the California Consumer Privacy Act or “CCPA”. This section of our statement is used to allow us to fulfill our CCPA obligations and explain your CCPA rights. For purposes of this section, the words “you” and “your” mean only such California residents.

What did we collect from California Residents?

We collect the following categories of personal information: identifiers such as name, address, IP address, and other similar identifiers; personal information described in subdivision (e) of Section 1798.80 (California customer records statute) such as a name, address, telephone number, credit card number; commercial information such as products or services purchased; internet/electronic activity such as browsing history and search history; geolocation data including geographic coordinates/physical location; and audio, video, electronic or other similar information. We may disclose this information for one or more business purposes permitted by the CCPA. We do not sell, and within the last 12 months have not sold, personal information to third parties.

Rights of California Residents

You have the following rights under the CCPA, in summary disclosure, access and delete. More information can be found here. It’s important to us that you know that if you exercise these rights, we will not “discriminate” against you by treating you differently from other California residents who use our sites and mobile resources or purchase our services but did not exercise their rights.

You can exercise these rights up to two different times every 12 months. To do so, just contact us contact@betterwaysaccounting.com. We may ask you to fill out a request form. The CCPA only allows us to act on your request if we can verify your identity or your authority to make the request so you will also need to follow our instructions for identity verification.

If you make a verifiable request per the above, we will confirm our

receipt and respond in the time frames prescribed by the CCPA.

THE EU GENERAL DATA PROTECTION REGULATION

We do collect or otherwise obtain personal information from data subjects located in the GDPR Jurisdictions. We fulfill our GDPR obligations with respect to our workforce/job applicants, our customers (and their own end-clients), and our vendors and business partners through a series of separate notices, contracts or other terms provided to them at the time, and in the manner and form, GDPR and local law within each GDPR Jurisdiction requires.

We describe, in the immediately following section of this statement, how we comply with the GDPR for personal information collected from visitors to and users of our online and mobile resources while they were in a GDPR Jurisdiction. Thus, for purposes of that section, the words “you” and “your” mean only such GDPR Jurisdiction-based visitors and users.

What do we collect from you in the GDPR Jurisdictions and how do we use it?

We collect from you the categories of personal information already described. The lawful basis on which we rely for such collection, later use and disclosure, is what the GDPR refers to as legitimate interest. As stated elsewhere in this statement, we do not sell any of your personal information to third parties nor do we use it for automated decision making.

Cross-border Data Transfers and Third-Party Processors

If we transfer personal information from the GDPR Jurisdictions to a location that has not been deemed by the European Commission to have adequate privacy protections, we do so in the manner the GDPR permits.

Rights of Data Subjects in the GDPR Jurisdictions

While we attempt to allow all visitors and users of our online and mobile resources to exercise a degree of control over their personal information, under the GDPR we have a legal obligation to do so for you. More specifically, with respect to personal information collected from you while you were in a GDPR Jurisdiction, you have these rights: transparency, access, correction and deletion, portability, who, what,

why and where, and restriction/objection (for more information click here).

If you would like to exercise any of these rights, please contact john@betterwaysaccounting.com. Your ability to exercise these rights is subject to certain conditions and exemptions that you can read about in Articles 12 through 23 of the GDPR. Among those conditions is our right to decline part or all of a request if we cannot satisfy our reasonable doubts and concerns about your identity in a manner that helps us minimize the risk that unauthorized persons might use a GDPR right to access your personal information. We will respond to all requests without undue delay, and in accordance with the time frames, if any, prescribed by the GDPR. If you are not satisfied with how we use your personal information or respond to your requests, you have the right to complain to your data protection regulator. Contact information for the EU data protection regulators can be found here.

RIGHTS OF DATA SUBJECTS IN OTHER JURISDICTIONS

In other jurisdictions, with similar data privacy regulations, we may collect from you the categories of personal information already described. We collect and manage (including disclose) such data in compliance with applicable local law(s). As noted, we do not sell any of your personal information to third parties nor do we use it for automated decision making.

CHANGES TO THIS PRIVACY STATEMENT

This privacy statement was drafted on January 1, 2022, and is effective as of this date. The English language version of this privacy statement is the controlling version regardless of any translation you may attempt.

We reserve the right to change or update this statement from time to time. Please check our online and mobile resources periodically for such changes since all information collected is subject to the statement in place at that time.

CONTACTING US

If you have questions about our privacy statement or privacy practices, please contact us at:

Better Ways Accounting & Tax

12020 N 35th Avenue Suite 108

Phoenix, AZ 85029

john@betterwaysaccounting.com

Note on how we can communicate with you:

By agreeing to our terms of service a prospect agrees to receive snail mail, email, phone and automated prerecorded voice message solicitations from Better Ways Accounting & Tax, including its various business divisions, affiliates, partners, vendors, list managers and clients who purchase our lists. You also agree to be contacted on a recurring basis for as long as you are a part of our sms/mms mobile message marketing program. We may sell the personal information that you supply to us and we may work with other third party businesses to bring selected retail opportunities to our members via direct mail, email, SMS, text and telemarketing (including but not limited to pre recorded phone messages). Filling out any forms on our pages constitutes my signature and agreement that the Better Ways Accounting & Tax and it's representatives, agents, and partners may contact me by telephone (including at my wireless telephone number), email, SMS, or pre-recorded message at the information I provided through this website, and I understand and agree that this consent applies even if my number is listed on a state or federal do-not-call list. By filling out any of our forms you also agree that you cannot "build a case" against Better Ways Accounting & Tax (by counting infractions per solicitation) because by submitting any forms or filling out any information signifies that you are requesting to be contacted by email, including SMS, text, pre-recorded phone calls. In no event shall either party be liable for special, indirect, incidental, or consequential damages, including, but not limited to, loss of use, or loss of profits.

Message and data rates may apply.

Prospect agrees he/she is solely responsible for any and all third party fees a prospect may incur when being contacted by Better Ways Accounting & Tax and its business divisions, affiliates, partners, clients, vendors and list managers. By filling out ANY of our forms you also forfeit your right to litigate against Better Ways Accounting & Tax based on any previously alleged infraction (alleged infractions prior to you submitting any forms) including but not limited to SMS, email, or robo-dial. If any of the terms are held unenforceable, the reminder of the

terms shall remain in effect.

Please DO NOT digitally sign this agreement by submitting any forms on any of our websites if you do not agree with our terms and conditions.

To unsubscribe from email, phone, sms, or robo-dialing mediums please send an email to contact@betterwaysaccounting.com and include the phone number and or email address you wish to be removed. You may also call and leave a message indicating such request at 602-880-1290, you can also opt-out by replying to the text message with “STOP”.

Better Ways Accounting & Tax - Our Data Retention Policy can be found here:

Data Retention and Destruction Policy

By John Love

Title: Data Retention and Destruction Policy	
Department: IT Department	**Version:** Original
Approved by: John Love, Owner	**Approval Date: January 1st, 2022**
Senior Management Approval: John Love, Owner	
Effective Date: January 1st, 2022	**Last Updated: January 1st, 2022**
Author: John Love, Owner	

Scope

This policy applies to the Arizona Location of Better Ways Accounting & Tax

12020 N 35th Avenue Ste 108
Phoenix, AZ 85029

Authority

This policy is hereby approved and authorized.

_____John Love_____	_____Owner_____	_____Jan 1st, 2022__
Name	Title	Date

Purpose

The purpose of this policy is to define the activities associated with the provision of data retention and destruction plans and programs that protect Better Ways Accounting & Tax's information systems, networks, data, databases and other information assets. Additional policies governing data management activities will be addressed separately.

Scope

The scope of this data retention and destruction policy is all information technology systems, software, databases, applications and network resources needed by the Company to conduct its business. The policy is applicable to all Company employees, contractors and other authorized third-party organizations.

Statement of Compliance

This policy is designed to be compliant with the U.S. Data Protection Act of 1998, Freedom of Information Act of 2000, Fair and Accurate Credit Transactions Act of 2003, Gramm-Leach-Bliley Act.

Data retention and destruction policy compliance is managed by the IT department, with support from Better Ways Accounting & Tax department leadership and subject matter experts. To achieve compliance, data retention and destruction programs must include appropriate procedures, and identify staffing and technology resources to meet compliance requirements. Compliance verification (especially for data destruction) is performed monthly by the IT department, internal audit or other appropriate entity.

Policy

The Information Technology (IT) department is responsible for managing all data retention and destruction activities for the Company. Other departments, such as Finance and Accounting, Operations and Human Resources, are also responsible for providing the IT department with their requirements for data retention and destruction. The IT department is responsible for developing, executing and periodically testing data retention and destruction procedures. The IT department also acknowledges it will comply with appropriate industry standards for data retention and destruction in its activities.

- The company shall develop comprehensive data retention and destruction plans in accordance with good data management practices as defined by established standards.
- Data retention and destruction activities shall be performed as part of the company's data management program, which administers and manages the overall technology data management program, which includes:
    - Planning and design of data retention and destruction activities;
    - Identification of data retention and destruction teams, defining their roles and responsibilities and ensuring they are properly trained and prepared to perform their duties;
    - Planning, design and documentation of data retention and destruction plans;
    - Scheduling of updates to data retention and destruction risk analyses;
    - Planning and delivery of awareness and training activities for employees and data retention and destruction team members;
    - Planning and execution of data retention and destruction plan exercises;
    - Designing and implementing data retention and destruction maintenance activities to ensure that plans are up to date and ready for use;
    - Preparing for management review and auditing of data retention and destruction plan(s); and
    - Planning and implementation of continuous improvement activities for data retention and destruction activities and plans.
- Formal risk assessments (RAs) and business impact analyses (BIAs) shall include requirements for data retention and destruction activities; RAs and BIAs shall be updated at least annually to ensure they are in alignment with the business and its technology requirements.
- Data retention and destruction plans shall address electronic data stored on electronic media such as CDs, hard disk drives, solid state disk drives, magnetic tape and other appropriate media.
- Data retention and destruction plans shall address data stored on non-electronic media (e.g., paper files, microfiche).
- Data retention and destruction plans shall address electronic information systems (e.g., servers, routers, switches) and components (e.g., cabling and connectors, power supplies, storage racks) and other assets that are currently out of production or scheduled to be phased out of production environments.
- Data retention plans shall establish the storage requirements and associated metrics (e.g., length of storage, type of storage media) for electronic and non-electronic information as well as systems supporting the IT infrastructure.
- Data destruction plans shall establish the parameters for destruction of electronic data (e.g., overwriting, reformatting, degaussing, firmware-based erasure, physical data media destruction), non-electronic data (e.g., shredding of hard copy), and systems and components (e.g., third-party destruction services).
- Data retention and destruction plans shall be periodically reviewed and tested in a suitable environment to ensure that data, databases, media, systems and other relevant elements can be retained or destroyed and that Better Ways Accounting & Tax management and employees understand how the plans are to be executed as well as their roles and responsibilities.
- All employees must be made aware of the data retention and destruction program and their own roles and responsibilities.
- Data retention and destruction plans and other documents are to be kept up to date and will reflect existing and changing circumstances.

Data Retention and Destruction Specifications

Following are specific data retention and destruction technical requirements:

General

- As our clients provide data for us to perform different accounting and tax preparation services we need to retain this data to ensure that the work was done correctly from the information provided. The output of the work will need to be retained as well. In accordance with generally accepted accounting practices for best practice, the input of the work and the output of the work need to be kept for 7 years after it was used by the client. This will allow us to verify the integrity of our work into the future and provide the client with what would be needed for the generally accepted time frame.
- After 7 years the data will be deleted. We will also delete all of the data at the request of our clients. We will also provide the data at the request of our clients as well.
- The IT Department is responsible for the data retention as well as the data destruction. The IT Department will follow their protocols to perform these actions and will continually be improving the protocols for both the retention and the deletion of this data.
- If there is a problem with the retention and deletion protocols, this issue will be immediately elevated the Owner of the organization, currently John Love.

Data/System Retention Procedures

- Currently the data is stored on our AWS production server and specific documents are stored on Google Drive.
- The systems are stored and maintained through GitHub as well as on the production server.
- The data systems are stored and maintained on the production server and on Google Drive.
- All of the data that is taken in from the client is stored on the production server and Google Drive. This is verified by the team as the data is used to output the final work. During this process it is verified that all necessary information is being stored correctly.
- The data is validated in conjunction with reviews of the work and the data directly with the client.

Data/System Destruction Procedures

- Data is destroyed 7 years after it is used by the client. This data includes the raw data from the client that is used to output the accounting work and the accounting work itself. We use the internal delete features on google drive and have procedures that delete the raw data from the production servers.
- Once the 7 year timeline has passed, the documents are deleted from Google drive using the built in deletion tools of google drive. The data is deleted from the production server through procedures that effectively delete the data.
- Once the data has been deleted it is verified by a member of the IT department who checks to see that the data can not be found and is no longer on the production server or in google drive.

Retention and Destruction Requests

- If a client is to request that the data is retained for beyond the 7 year time period, we allow them to do this and assist in keeping the data around longer.
- If a client is to delete their account they are given the option of deleting the data that we hold. The client can also request this be done without deleting their account.
- If the client would like access to all the data we hold, we provide them with the data through a folder in google drive where all their documents are kept as well as any information about them on the production server.

Policy Leadership

John Love, Owner is designated as the corporate owner responsible for data/system retention and destruction activities for the Company. Resolution of issues in the support of data/system retention and destruction activities should be coordinated with IT management and others as needed.

Policy Responsibilities

- Policy Approval – The Owner is responsible for approving this policy.
- Policy Implementation – The IT Department is responsible for planning, organizing and implementing all activities that fulfill this policy.
- Policy Maintenance and Updating – The IT Department is responsible for all activities associated with maintaining and updating this policy.
- Policy Monitoring and Review – The Owner is responsible for monitoring and reviewing this policy.
- Policy Improvement – The Owner and the IT Department are responsible for defining and implementing activities that will improve this policy.

Management Review

The Owner will review and update this data retention and destruction policy on an annual basis. As changes to this policy are indicated in the course of business, the Owner may initiate a change management process to update this policy.

Policy Enforcement

The Owner will enforce this policy.

Penalties for Noncompliance

In situations where it is determined that data retention and destruction activities do not comply with this policy, the IT department team assigned to this activity will prepare a report stating the reason(s) for noncompliance and present it to IT management for resolution. Failure to comply with this data retention and destruction policy within the allotted time for resolution may result in verbal reprimands, notes in personnel files, termination, and such other remedies as deemed appropriate.

Policy Location

The policy will be signed, scanned into an electronic file and posted in the following location on the network: https://docs.google.com/document/d/1fGvJVXrXrBGdr5CXTBl_V40b9LJ10ks4/edit?usp=share_link&ouid=116839131792731615116&rtpof=true&sd=true