Mindful Tax

**Data Security and Cybersecurity Program**

Revised as of 10/2023

Introduction

**Objective**

Our objective, in the development and implementation of this Data Security Program (“the Program”), is to create effective administrative, technical, and physical safeguards for the protection of personal information of our clients, our employees, and proprietary data of Mindful Tax. This program sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting sensitive data. The Program complements Mindful Tax’s existing Business Continuity Plan and Privacy Policy.

**Purpose**

The purpose of the Program is to:

1. Ensure the security and confidentiality of personal information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of theft or fraud.

**Scope**

In formulating and implementing the Program, we will:

1. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information;
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
3. Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. Design and implement a Program that puts safeguards in place to minimize those risks, consistent with Federal and State laws; and
5. Regularly monitor the effectiveness of those safeguards.

**Data Security Coordinator**

We have designated Meghan Lape to implement, supervise, and maintain the Program. That designated employee (the “Data Security Coordinator”) will be responsible for:

1. Initial implementation of the Program;
2. Training employees;
3. Regular testing of the Program’s safeguards;
4. Evaluating the ability of each of our third-party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access and requiring such third-party service providers by contract to implement and maintain appropriate security measures;
5. Reviewing the scope of the security measures in the Program at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information;
6. Conducting an annual training session for all relevant staff, including temporary and contract employees who have access to personal information on the elements of the Program. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with Mindful Tax’s requirements for ensuring the protection of personal information.

Data Security Program

## Risk Identification and Assessment

**Background:** Classifying data according to its sensitivity level is a common practice that provides insight into how certain data should be protected across a firm. Adequately protecting data according to its classification level reduces risk and supports the appropriate allocation of resources (e.g., resources are not spent “overprotecting” low-risk data).

**Risk Identification:** Mindful Tax conducts a risk assessment reasonably designed to identify foreseeable internal and external risks to the security, confidentiality, and integrity of data and the systems used by Mindful Tax and critical third-parties to process that data, where such risks could result in the unauthorized disclosure, misuse, alteration, or destruction of that information or those systems. This risk assessment includes the following:

* **Data Inventory** – This is completed to detail what data Mindful Tax has, where it is kept, how it is protected, and who can access it.
* **Data Classification** – Data classification is one of the most important steps in data security. Not all data is created equal, and few businesses have the time or resources to provide maximum protection to all of their data. In order to understand what our most sensitive data is, where it is, and how well it is protected, Mindful Tax has applied to following data classifications:
  + **HIGHLY CONFIDENTIAL** – This applies to the most sensitive business information that is *intended strictly for use within Mindful Tax.* *Its unauthorized disclosure could seriously and adversely* impact Mindful Tax, business partners, vendors, and clients. This includes, but not limited to:
    - Personal Information of Clients and employees,
    - Employee payroll files,
    - Social Security Numbers,
    - Account Numbers
  + **SENSITIVE** – This classification applies to sensitive business information that is intended for use within Mindful Tax, and information that would be considered to be private. This includes, but not limited to:
    - Employee performance evaluations,
    - Internal Audit Reports
    - Financial Reports
    - Partnership Agreements
    - Marketing Plans
  + **INTERNAL USE ONLY** – This classification applies to sensitive information that is generally accessible by a wide audience and is intended for use only within Mindful Tax. While its unauthorized disclosure to outsiders is against policy and may be harmful, it is not expected to impact Mindful Tax, employees, business partners, vendors, etc.
* **Security Control Analysis** – Analyze how Mindful Tax protects its systems, identify security weaknesses, and create remediation plan.

**Evaluation:** Mindful Tax evaluates the Date Security Program, on at least an annual basis, based on the following:

* Those matters identified as material risks in the Risk Assessment;
* Relevant changes in technology and business processes, if any;
* Any material changes in or to Mindful Tax’s operations or business arrangements, including any material change in technology or technology-based services provided by a Vendor; and
* Any other circumstance that Mindful Tax reasonably believes may have a material impact on the Program.

In addition, Mindful Tax will not implement a material enhancement to the technology it utilizes (regardless of whether it is maintained by Mindful Tax or by a Vendor) to conduct its principal business until and unless Mindful Tax determines that the enhancement will not result in unreasonable risk of creating a weakness in the Program.

**Risk Assessment Statement:** Mindful Tax has developed and implemented the following safeguards intended reasonably to mitigate the risks identified in the Risk Assessment.

* Mindful Tax has implemented technology (directly or through Vendors), including Drake Tax and Drake Portals that are capable of being used securely. Mindful Tax maintains a written list of the technology that it utilizes, including technology provided by Vendors to which Mindful Tax has outsourced processing and related functions.
* Mindful Tax monitors the use of technology it utilizes, and the scope of that monitoring is designed to identify any interruptions in the use of such technology. In particular, Mindful Tax’s monitoring processes include the following:
  + Implementation and monitoring of frequent password changes, locking of devices, and reporting of lost or stolen devices;
  + Technology/device access is routinely audited and updated appropriately;
  + Devices are routinely backed up; and
  + Implementation, use, and monitoring of anti-virus software on all devices.
* Mindful Tax implements the appropriate encryption standard as recommended by technology it utilizes and its vendors.
* Mindful Tax has established access controls to its network(s), including by providing identities and credentials for authorized users and monitoring those identities and credentials. Employee credentials are required to be updated quarterly. The DSC controls access to Mindful Tax networks and sets up new authorized users.
* Mindful Tax has created a written authentication process to enroll and verify any authorized user(s) of technology provided by Mindful Tax. The authentication process is supervised by the DSC and consists of issuing access to new authorized users when needed, maintaining a list of authorized users for each separate technology, removing users when needed, and reviewing the authorized user list annually.

Mindful Tax, with respect to technology that it maintains at its office, continuously monitors its technology and networks for indications of an intrusion. This monitoring is supervised by the Data Security Coordinator and consists of using anti-virus software on all devices accessing the Firm’s network and/or technology; ensuring software updates are completed on a regular basis, and that an appropriate firewall is used. Additionally, Mindful Tax has reviewed the monitoring processes employed by each of the relevant Vendors, with respect to technology-based processes outsourced to the Vendor(s) by Mindful Tax and intends to regularly seek updates from the relevant Vendors regarding any material changes in their respective monitoring processes.

**Vendors: Mindful Tax** has taken the following actions intended to identify potential weaknesses and vulnerabilities in the Program as a result of Mindful Tax’s reliance on technology-based processes maintained by Vendors:

* Mindful Tax has evaluated existing safeguards which restrict access by employees and third- parties to technology provided by Vendors;
* Before Mindful Tax selects a Vendor, it reviews the prospective Vendor’s information security protocols and protections relative to Mindful Tax’s due diligence standards; and
* Mindful Tax monitors Vendors for indications of any security lapses or interruptions relating to networks and data maintained by those Vendors.

**Testing:** No less than once per calendar year, Data Security Coordinator will conduct, or arrange for a third-party to conduct, a test of the Program to identify any vulnerabilities. The results of the test will be summarized in writing.

## Website Security

**Background:** Web application vulnerabilities account for the largest portion of attacks outside of malware. It is crucial that any web application be assessed for vulnerabilities and that any identified vulnerabilities be remediated prior to use. For data collected through a website hosted by a third party, it is important to be sure the third party protects that data fully.

**Policy:** In addition to the existing safeguards in place, Mindful Tax has deployed the following to prevent unauthorized access to client data or accounts through the use of its public website:

* Deploy user authentication to identify approved users, digital signatures and other cryptographic mechanisms as appropriate.
* Use intrusion detection systems, intrusion prevention systems, and file integrity checkers to spot intrusions and verify web content.

## Password Protection Policy

**Background:** Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Mindful Tax's resources. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

**Policy:** All users, including contractors and vendors with access to Mindful Tax systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

* Password Creation
  + All user-level and system-level passwords must conform to the Password Construction Guidelines.
  + Users must not use the same password for Mindful Tax accounts as for other non-Mindful Tax access (for example, personal ISP account, online banking, benefits, and so on).
  + Where possible, users must not use the same password for various Mindful Tax access needs.
* Password Change
  + All system-level passwords (for example, root, enable, admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
  + All user-level passwords (for example, email, web, desktop computer, and so on) must be changed on at least a quarterly basis.
* Password Protection
  + Passwords must not be shared with anyone. All passwords are to be treated as sensitive, highly confidential Mindful Tax information.
  + Passwords must not be inserted into email messages or other forms of electronic communication.
  + Passwords must not be revealed over the phone to anyone.
  + Do not reveal a password on questionnaires or security forms.
  + Do not hint at the format of a password (for example, "my family name").
  + Do not share Mindful Tax passwords with anyone, including administrative assistants, managers, co-workers while on vacation, and family members.
  + Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
  + Do not use the "Remember Password" feature of applications (for example, web browsers).
  + Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Employee Training

No less than once per year, Data Security Coordinator (or a third-party retained by Mindful Tax) will train relevant staff regarding the primary elements of the Program. The training will cover, at a minimum, Mindful Tax’s legal and regulatory obligations to protect Personal Information, and a summary of the elements of the Program intended to safeguard such Personal Information.

Data on the Move

## Email Usage Policy

**Background:** Electronic email is pervasively used and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it’s important for employees to understand the appropriate use of electronic communications.

**Policy:** This policy covers appropriate use of any email sent from a Mindful Tax email address and applies to all employees and agents operating on behalf of Mindful Tax.

All use of email must be consistent with Mindful Tax policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

Mindful Tax email account should be used primarily for Mindful Tax business-related purposes; personal communication is permitted on a limited basis, but non-Mindful Tax related commercial uses are prohibited.

* All devices that provide for access to email, including but not limited to, desk top computers, laptops, mobile phones, and tablets, require authentication practices that include password access. Passwords are changed quarterly.
* Email that is identified as a Mindful Tax business record shall be retained according to Mindful Tax Record Retention Schedule.
* Users are prohibited from automatically forwarding Mindful Tax email to an unapproved third-party email system. Individual messages which are forwarded by the user must not contain Mindful Tax “Sensitive” or above information.
* Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Mindful Tax business, to create or memorialize any binding transactions, or to store or retain email on behalf of Mindful Tax.  Such communications and transactions should be conducted through proper channels using Mindful Tax-approved documentation.

## Mobile Computing

**Policy:** In order to have access to Mindful Tax or client data, the following safeguards must be implemented on mobile devices, such as smartphones and tablets:

* **Password Protection** -4 digit pin or password.
* **Remote Locate and Wipe -** Have the ability to remotely locate and wipe the device if it is lost. There are apps such as Android Device Manager, Avast or FindMyPhone that allow users to remotely wipe a device if it is lost. This is the final measure of protection mandated by our procedures.

## Public Wi-Fi

Public Wi-Fi such as free wireless at airports, hotels and businesses is inherently dangerous and should be avoided if possible. It is recommended to use your mobile phone as a secure mobile hotspot or setup a Virtual Private Network (VPN) if you must use a public Wi-Fi access point. There are free services, such as “Hotspot Shield”.

Facility Security

## Clean Desk Policy

**Background:** A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an employee workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace.

**Policy:** This policy applies to all Mindful Tax’s employees and requires:

* Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
* Computer workstations must be locked when workspace is unoccupied.
* Computer workstations must be shut completely down at the end of the workday.
* Any highly confidential or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
* File cabinets containing highly confidential or sensitive information must be kept closed and locked when not in use or when not attended.
* Keys used for access to highly confidential or sensitive information must not be left at an unattended desk.
* Portable computing devices such as laptops and tablets must be either locked with a locking cable or locked away in a drawer.
* Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
* Printouts containing highly confidential or sensitive information should be immediately removed from the printer.
* Upon disposal, highly confidential and/or sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
* Whiteboards containing highly confidential and/or sensitive information should be erased.
* Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

## Mail Security

**Policy:** Mindful Tax utilizes a locked mailbox for sending and receiving mail.

## Trash Disposal

**Policy:** All documents that contain sensitive information must be disposed of by use of shredder/shred bin (in the event of a shredding vendor). Shred bins are locked and emptied on a sufficient frequency.

## Electronic Equipment Disposal

Policy:Disposing of electronic equipment requires skilled specialists in order to ensure the security of sensitive information contained within that equipment. When electronic equipment (i.e. computers, mobile phones, tablets, etc.) is retired from service, outside professional help, such as an experienced electronic equipment recycler and data security vendor, will be obtained to remove personally identifiable and sensitive data.

Incident Response and Reporting

Mindful Tax has implemented the following procedures for responding to an incident involving unauthorized access to, or unauthorized disclosure or use of, Personal Information:

* The Data Security Coordinator will direct the assessment of the nature and scope of any such incident, including the circumstances which led to the detection of the intrusion, and will identify the systems, networks, and data involved in the incident;
* On the basis of the Data Security Coordinator’s assessment, the Data Security Coordinator will direct and supervise the actions taken by Mindful Tax to contain and control the incident to prevent further unauthorized access to, or unauthorized disclosure or use of, Personal Information; and
* The Data Security Coordinator will conduct (or direct and supervise) a prompt investigation of the incident, with the objective of determining the likelihood that Personal Information has been or will be misappropriated;

The Data Security Coordinator will document Mindful Tax’s actions taken in response to each incident, including any assessment of the nature of what occurred, how Mindful Tax responded to the incident, the scope of any misappropriation of Personal Information, and the action(s), if any, Mindful Tax intends to take to prevent any future incident.