Holistiplan's IT Security Best Practices

Last Updated: 11/14/2022

Company Overview & Operations

Corporate Address: 3193 Chaco Canyon Drive, College Station, TX 77845
Corporate Phone Number: 979-217-1281
Website: www.holistiplan.com
Prospective Customer Information Contact: info@holistiplan.com
Application/Technical Assistance: support@holistiplan.com

Does Holistiplan provide cloud service(s)?
Yes, Holistiplan's tax software is completely cloud-based. Our solution is offered as a SaaS tool and leverages industry-leading technology through our partnership with Amazon Web Services (AWS). While our service is multi-tenant, AWS leverages tenant isolation so that our data is kept entirely separate and is not accessible to anyone outside of the Holistiplan organization.

Does Holistiplan retain our data?
This is under the subscriber's control. Holistiplan will retain the data until that data is deleted by the subscriber or until the subscriber cancels their subscription. Holistiplan retains the uploaded PDF in a secure, encrypted drive. Some data, used for analysis and calculations, is read off of the PDF and stored within the Holistiplan application itself. This data includes:

- Taxpayer's Full Name
- Taxpayer's Income, as Recorded on the Tax Return

The types of data we collect on your organization are:

- Name of Organization
- Email Information
- Payment Information (via Stripe, a third party payments provider - Holistiplan staff does not have access to payment information)

Holistiplan User Access Management

How many staff members does Holistiplan currently employ?

Holistiplan is a small but effective team. Across approximately 30 team members, roughly one-third are in product development, one third are in support, and the remainder are split between sales, marketing and administration. All support staff are company employees (no contractors). We take security seriously and have employed a consulting CISO to evaluate our security posture as it relates to our application and protecting our customers' critical data.

Does Holistiplan require your staff to be trained and tested on information security protection and cybersecurity policies and procedures?

Yes, all employees are required to complete a security awareness training at time of hire, as well as on an annual basis thereafter. This training includes topics such as threats to be aware of, strategies for remaining safe, phishing, and clean desk policy.

How often does Holistiplan review employee access and privileges?

Access management is a core discipline and is managed and monitored for compliance with the Soc 2 Type II reporting framework. This includes quarterly access reviews. The principle of least privilege is employed.

Has Holistiplan conducted background checks on all individuals with privileged access?

Yes. In accordance with SOC 2 Type II, we run background checks on employees prior to granting them any privileged access in Holistiplan's IT environment.

Does Holistiplan have a disciplinary process for noncompliance with information security policies?

Yes, as part of our corporate information security program and employee handbook policies.

Does Holistiplan have a process to block terminated staff from accessing systems and data?

Yes. In addition to our User Access Review process, we have a formal termination process for all employees/contractors that have departed the company. Their access is removed from our Holistiplan system (if applicable) immediately. There is a formal checklist in place with defined timelines that are monitored and must be met to remain compliant with SOC 2 Type II.

Does Holistiplan have a process to adjust staff access to systems and data when there is a change in staff status and someone undertakes a new role?

Yes, as part of our SOC 2 access management policy/practices.

What tools do I have available in your application to increase my data security?
Holistiplan offers Multi-Factor Authentication. Using this, should your password be compromised, a bad actor would not be able to access your data without possession of your second authentication factor, in this case a rotating code produced by an app on your smartphone. In addition, your firm will have control over session lifespan to ensure that access to the application is prevented without re authenticating after a period of inactivity. For all users, a rigorous password policy is in place to prevent use of weak passwords, password reuse, and ensure password complexity. Your firm may also opt to customize the “too many failed attempts” setting that prevents login when an incorrect password has been used too many times in a timeframe.

Holistiplan Internal IT Compliance Program

Does Holistiplan have an internal compliance and/or ethics program?

Yes. Holistiplan’s Security Program is informed by SOC 2 Type II and NIST frameworks, and is continuously monitored for control effectiveness using a number of technical tools and processes. Conduct and ethics are covered within this security and compliance program.

Does Holistiplan maintain policies and procedures to enable compliance with legal, regulatory, statutory, or contractual obligations regarding information security requirements?

Yes, Holistiplan has extensive documented policies and procedures in place that are designed to support SOC 2 Type II compliance. Holistiplan monitors for compliance and undergoes regular SOC 2 audits.

Will your company market, sell or interact directly with our firm’s clients?

No.

Does Holistiplan have an operational change management policy or program approved by management and communicated to appropriate constituents?

Yes. Holisitplan’s Operations Security Policy contains a Change Management component and is reviewed by management on at least an annual basis.

Who or what department is responsible for maintaining and reviewing this program?

The Holistiplan executive management, including the CTO, vCISO and co-founders are responsible for maintaining and reviewing the Change Management Program.

Does Holistiplan have a data classification and retention program for client data that identifies the data types requiring additional management and governance?

Yes. Holistiplan has a documented data classification model incorporated in its data management policies. All customer data is restricted under the most sensitive classification.

Holistiplan Privacy Program

Does Holistiplan have a documented privacy program with administrative, technical, and physical safeguards to protect client data?

Yes. Our Privacy Program is outlined on our website and incorporated in Holisitplan’s extensive policies and procedures that safeguard client data.

For client data, Does Holistiplan have a dedicated person or group responsible for privacy compliance?

Yes, Holistiplan’s CTO works in conjunction with the company’s consulting CISO to maintain our compliance and security standards as they relate to data privacy.

Does Holistiplan have a documented response program to address privacy incidents, unauthorized disclosure, unauthorized access, or breach of client data?

Yes, Holistiplan has incorporated its formalized incident response program in its information security policies and procedures. It is tested annually.

Does Holistiplan store any data outside of the United States?

No. Including any backup copies, all data remain in data centers within the United States.

Holistiplan Backups Policy

Does Holistiplan encrypt our data?

Yes, Holistiplan encrypts all data within our application both at rest and in transit. We leverage industry-leading 256 bit encryption.

Are system backups of the Holistiplan client systems and client data performed?

Yes, we back up all critical systems and data to an alternative AWS cloud environment. We have the ability to call upon multiple instances and can recover to a specific point in time without significant loss or disruption. All of our backups are validated, stored and encrypted.

What controls/security measures does Holistiplan implement to maintain security for workstations/mobile devices?

Although customer data are not stored or processed on employee workstations or devices, employee devices are managed by a central management system and monitored for non-compliant status. In order to ensure protection of client data, Holistiplan has implemented a variety of security measures, including: multi-factor authentication, password protection on the endpoint, endpoint encryption, screen-lock timeouts, anti-malware, remote wipe capability, protection of the physical device itself, endpoint protection and monitoring, and encryption of the data stored in our servers. Rigorous strong-password policies are in place. All access to client data is logged, whether by the customer or by internal Holistiplan staff. Furthermore, our team uses proper security hygiene when interacting with client data and Holistiplan ensures that only users who require access to fulfill their job responsibilities are able to interact with client data.

Holistiplan Third Party Management

Do external parties (including back-up vendors, service providers, equipment maintenance vendors, software maintenance vendors, data recovery vendors, etc.) have access to client systems and client data or processing facilities?

No. While Holistiplan leverages Amazon Web Services, access to data on their hardware is accessible to Holistiplan only.

Does Holistiplan share our data with third party vendors?

No, we do not share your firm’s or your client’s data with any outside entities. Per our privacy policies, we would only share information if compelled to do so by law enforcement.

Does Holistiplan have employment contracts in place to address the privacy and security requirements of the services provided?

Yes, we require all employees to sign a confidentiality agreement that specifically protects subscribers and subscribers’ clients’ data.

Does Holistiplan have a process to ensure that any personal information provided by individuals or clients is limited for the purposes described in the respondent’s privacy notice?

Yes, Holistiplan maintains a Privacy Policy for all of our customers and we as an organization ensure that the personal information collected is never used outside of the scope of our business service or our Privacy Policy.

Does Holistiplan have documented policies, procedures, and controls to limit access based on need to know or the minimum necessary for constituents?

Yes, we formalized and documented logical access policies that capture best practices such as least privilege access, preventing shared logins, user authentication methodologies, access reviews, and restriction of privileged account use.

Does Holistiplan regularly monitor your staff, vendors, and business partners for privacy compliance?

Yes. With the security measures we have in place (as outlined above), we have stringent measures in place to control the privacy of sensitive data as it relates to our organization and that of our customers. We actively limit the access for all employees to critical systems and align their access with their job responsibilities. Contractors do not receive access to client data.

Does Holistiplan fully control the physical machines and access to those machines that host data and systems utilized for clients?

Due to our unique cloud environment, our application and associated data are purely SaaS based, meaning all data are stored in the AWS cloud. As such, we do not maintain physical machines, thereby mitigating the risk of exposing our physical hardware to vulnerabilities.

What are your requirements to ensure password complexity?

Holistiplan has implemented a password policy that ensures the use of strong passwords. This includes validations such as preventing use of common passwords, preventing reuse of passwords, preventing use of passwords similar to user attributes such as username or email, requiring that passwords have at least 12 characters, a minimum number of differing characters, use of symbols, numbers, and different capitalization. Holistiplan is continually reviewing best practices and taking feedback from customers, so the specific parameters continue to evolve.

Does Holistiplan permit remote access for your employees/contractors?

Yes. Since the application itself is cloud-based, all employees and contractors technically work remotely.

We incorporate best practices around Identity & Access Management for all critical systems. Multi-Factor Authentication is in place for all employees. Any access of client data is done through an encrypted connection. Furthermore, we do not manage an on-prem application or network and therefore limit our exposure as it relates to employees/contractors.

Holistiplan Data Center Best Practices

What physical safeguards Does Holistiplan have in place to protect your data center and your business?

Holistiplan operates purely in a cloud environment using AWS services. As such, the security safeguards required to protect the data center are managed by Amazon. Amazon maintains stringent security parameters around their data centers and obtains industry-leading compliance certifications, such as SOC1-2 and ISO 27001. From redundancy to third-party audit attestations, AWS has some of the most stringent security standards in the world.

Does Holistiplan review AWS's security posture on a periodic basis?

Yes, as part of our SOC2 compliance, Holistiplan receives and reviews AWS's SOC2 report on an annual basis.

What type of vulnerability and infrastructure penetration testing does Holistiplan use to gauge threats from outsiders as well as from those with inside information about the system?

Our Holistiplan application is continuously monitored and reviewed for availability, confidentiality and integrity. Holistiplan operates purely in the cloud and does not have a dedicated corporate network. As such, our protection parameters are enforced in our cloud environment, at the application level, through our private connections to our shared workspace network, and at the endpoint level (our workstations). Holistiplan uses a suite of SIEM tools to do regular penetration testing and monitor configuration changes, system or configuration vulnerabilities, or other anomalies such as unusual user/administrator behavior. An intrusion detection platform is also in continuous use. In addition, the application is protected by a Web Application Firewall.

Does Holistiplan provide, support, host, or maintain web services that have access to client systems?

No. Our service is completely maintained by Holistiplan and does not connect to client systems.

Does Holistiplan have an intrusion detection system for potential data security breaches?

Yes, as part of our services with AWS, Holistiplan has monitoring tools in place to detect anomalous behavior, including intrusion, in our cloud environment.

Does Holistiplan use wireless networking?

Holistiplan prohibits wireless networking in its environment.

Holistiplan Vulnerability Best Practices

Does Holistiplan have an antivirus/malware policy or program (for workstations, servers, and mobile devices) approved by management and communicated to appropriate constituents?

Yes, Holistiplan maintains a formal antivirus/malware program as part of its documented information security policies. Devices are monitored for compliance.

What security protections does Holistiplan have in place in order to protect Holistiplan's servers?

We employ a broad suite of tools offered by AWS to protect our servers. This spans across the infrastructure and the application, protecting the application with multiple types of firewalls (including a Web Application Firewall), ongoing automated monitoring for any vulnerabilities, change management, logging and monitoring administrator activity within the environment, and more. A patch management system continually monitors for security patches, and we complete third party penetration tests at least annually.

Does Holistiplan have security patches in place to ensure the Holistiplan system always operates on the most current version?

Yes, our application is continuously developed and enhanced to maintain robust security measures, and the infrastructure on which it runs is maintained through a comprehensive patch management system that monitors for available patches multiple times per day. In addition, any components used within the code for the application are continually monitored by a system that alerts us when there is a security-related issue or patch for any of those components. All changes are tested in a non-production environment to mitigate the risk of creating vulnerabilities. Vulnerabilities are patched according to internal policy timelines according to severity.

Holistiplan Application Security Best Practices

Does your firm utilize a formal software development life cycle (SDLC) process or other methodology which ensures early and consistent consideration of security issues?

Yes, as part of our SOC 2 Type II compliant operations, our development organization operates according to the company's established Secure Development Policy. This includes a standardized process that focuses on best practices and workflow controls to ensure all software updates are reviewed and have passed internally-established standards based upon industry best practices.

Does Holistiplan maintain separate development and production environments?

Yes, Holistiplan operates production and staging environments as distinct from any development environments. Development and production are wholly separated. Client documents do not leave the production environment at any time. All changes are developed in a non-production environment and undergo validation, review, testing and approval by management prior to being deployed to production. Software deployment (releases) are done at such time and in such a way as to minimize disruption to users.

Does Holistiplan use SSL encryption to protect data transfers between a user's browser and the application?

Yes, all connections to our application established an encrypted connection using TLS 1.2 (with only ECDHE and SHA256 or stronger (384) ciphers). Perfect forward secrecy is supported.

Does Holistiplan use application penetration testing to simulate bad-actor situations?

Yes, Holistiplan hires a third party to conduct penetration testing on at least an annual basis in order to address any potential vulnerabilities. In addition, automated vulnerability analysis tools are employed on a perpetual basis, and AI tools are used to analyze the application code for vulnerabilities.

Holistiplan Data Loss Prevention Measures

Does Holistiplan have specific controls and information practices in place to address data loss, leak or both?

Yes, we enforce a variety of security best practices in order to prevent data loss and data leakage within our organization. At the core of this is extensive, auditable logging and monitoring.

Does Holistiplan utilize any applications/software for monitoring and restricting access or changes to data files, especially client data?

An extensive audit trail is in place to record every occasion upon which a customer data item is accessed by anyone, including internal Holistiplan employees, and whether that access event be through the Holistiplan application or through the infrastructure directly. Holistiplan actively enforces its stringent Access Management policies to ensure that client data can only be accessed by employees who require the access per their job responsibilities. In addition, Holistiplan uses tools to monitor any changes to configurations or permissions throughout the environment.

Has Holistiplan ever experienced any client data loss or theft?

No; in the history of our organization, we have never experienced a breach or been forced to report a compromise to authorities.

Holistiplan Business Continuity & Disaster Recovery Measures

Does Holistiplan have a Disaster Recovery Plan in place?

Holistiplan has extensive redundancy and backup capabilities built into our SaaS application. Geographic redundancy and real-time replication are in place. In the event of a disruption, we have the ability to resume service without significant interruption for our clients. Alongside these capabilities, a formalized business continuity policy is in place.

What type(s) of insurance coverage does Holistiplan have in place?

Holistiplan has the following insurance coverages in place:

- Professional liability (errors and omissions) insurance
- Network risk/cybersecurity insurance
- Insurance coverage for business interruptions or general services interruptions

Does Holistiplan have a security incident response plan in place?

Yes, Holistiplan has an established formalized incident response plan. We review this plan on at least an annual basis to ensure continued relevance and effectiveness. Furthermore, we conduct periodic incident response exercises to ensure our team understands their roles in the event of an actual incident. Fortunately, we have not been required to initiate our Incident Response Plan since the inception of our company.

Does Holistiplan notify your clients of security incident outcomes once your recovery measures have been completed?

Yes, Holistiplan's policy is that all clients are to be notified within 72 hours of the discovery of a breach that may have potentially impacted their services and/or data.

Holistiplan's Use of Contractors

Does Holistiplan employ contractors that have access to our firm and client data?

Holistiplan does not presently employ contractors to fulfill any roles that involve access to client data.