Tabitop's Security Policy

Effective February 24, 2014

Security Access

Tabitop's world-class, highly secure network of data centers and infrastructure utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7x365 by trained security guards, and authorized access is highly restricted. Tabitop's infrastructure and systems are also designed to minimize the impact of disruptions to operations, including redundancy across multiple geographic regions and data centers. This architecture allows Tabitop to remain reliant in the event of failure events, including natural disasters and/or system failures.

Tabitop's virtual infrastructure has been designed to provide optimum availability, while ensuring complete user privacy and isolation. Tabitop also balances a high level of security protocol, combined with a noteworthy layer of simplicity within our management console, which provides both a safe yet seamless user experience without sacrificing data and infrastructure security and reliability.

Each Tabitop virtual desktop PC instance is created, maintained, and operated as its own separate and virtually dedicated cloud-based computer system. The result of our infrastructure and service design allows each of our users the ability to fully customize, manage, and secure their own individual virtual desktop PC instance(s). This helps ensure that each Tabitop virtual desktop PC is isolated in its own micro-network and is also individually secured through a combination of both internal and external firewall protocol.

Data Encryption

Tabitop's virtual desktop infrastructure has been designed and built to be one of the most seamless and secure cloud computing environments available in the marketplace. Tabitop's infrastructure is built through a combination of highly secure third-party cloud providers as well as Advanced Encryption Standard (AES) 256 encryption technology. Tabitop provides an extremely scalable, highly reliable platform that enables users

to deploy, access, and manage virtual desktop PC instances (cloud-based computer systems), applications and data quickly and securely.

Security Features

Not only are Tabitop's user data and virtual desktop PC instances protected by highly secure facilities and infrastructure, but are also protected by extensive network and security monitoring systems. These systems provide basic but important security measures such as distributed denial of service (DDoS) protection, password brute-force detection, and Advanced Encryption Standard (AES) 256 encryption protocol. Additional security measures included with every Tabitop instance and subscription include:

- Secure Access – User access points, also called API endpoints, allow secure HTTP access (HTTPS) so that Tabitop users can establish secure communication sessions with each Tabitop Account and Desktops using SSL encryption and secure account access.

- Automated Firewalls – All Tabitop Virtual Desktop PC instances are protected by Tabitop's built-in firewall rules, which only allow remote desktop protocol (RDP) port access via alternating or dynamic Public IP address. This helps safeguard that no other unwanted or malicious traffic can access your Tabitop virtual desktop PC via standard open firewall traffic.

- Private Intranet– Although Tabitop users may be placed on similar internal networks, subnets, and infrastructure locations as other Tabitop users, Tabitop's firewall security protocol prohibits any other Tabitop PC from communicating or accessing other PC's via internal IP address protocol, unless the Tabitop subscriber purchases/manages multiple Tabitop PC subscriptions and requests access between instances directly. Tabitop also recommends leaving the pre-configured Windows Firewall settings enabled in order to maintain additional layers of security for each Tabitop desktop instance.

- Encryption – Tabitop stores all user data and instance storage in a secure infrastructure, which is encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption

standard using 256-bit encryption keys.

- Rotating Public IP Address – Because Tabitop virtual desktop PC instances are turned “On” and “Off” based on user usage needs, Tabitop adds an additional layer of automated security, wherein each Tabitop PC instance receives a new Private and Public IP address with each “On”/”Off” event. This discourages malicious services and attacks from being able to find a user’s specific Public IP address since it is constantly rotating in a randomized fashion. Tabitop’s secure protocol remains seamless to the user and is encrypted through the user’s account.

- Rotating Credentials – Tabitop also institutes best practices for creating and changing alternating administrative passwords that are unique and encrypted for each individual virtual desktop PC instance. This helps assure more stringent password credential policies for each desktop connection, of which is encrypted with Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys, via the Tabitop mobile app, and inaccessible from other remote connection software and services, giving each user a secured virtual desktop device.

- Never Store Password – Tabitop encrypts each user account password with Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys. No employee, agent, or entity will ever have access to your account password, and if users lose their password, they will need to reset via the Tabitop reset password web application as Tabitop is unable to recover account passwords or Tabitop’s virtual desktop PC instance administrative password as both are encrypted.

- VPN Connection Option – The Tabitop virtual desktop PC instance allows and supports users to establish a VPN connection with their office and/or home premise via third-party installed VPN clients and/or SSL VPN software. This connectivity option allows Tabitop virtual desktop PC instances to directly connect to a user’s existing home and/or office network securely.

Because the Tabitop's cloud infrastructure provides so many built-in security features, users are able to simply focus on the security of the user's individual virtual desktop PC and its applications. Tabitop always recommends assuring that each virtual desktop PC, its OS, and programs are always updated with the latest virus and spyware detection.

Tabitop Specific Security and Certifications

Tabitop's trusted third-party cloud partner(s)' certifications and evaluations have achieved ISO 27001 certification and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). Our cloud partners have undergone annual SOC 1 audits and have been successfully evaluated at the Moderate level for Federal government systems as well as DIACAP Level 2 for DoD systems.

Each of these partner certifications means that an auditor has verified that specific security controls are in place and operating as intended. Users can view the applicable compliance reports by contacting a Tabitop representative.

Third-Party Attestations, Reports and Certifications

HIPAA

Tabitop's trusted third-party cloud partner(s) enable covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure Tabitop environment to process, maintain, and store protected health information and Tabitop can sign business associate agreements with such customers.

Tabitop also offers a HIPAA-focused whitepaper for customers interested in learning more about how they can leverage Tabitop for the processing and storage of health information. The Creating HIPAA-Compliant Medical Data Applications with Tabitop whitepaper outlines how companies can use Tabitop to process systems that facilitate HIPAA and HITECH compliance. For more information on the Tabitop HIPAA compliance program please contact Tabitop Sales and Business Development.

SOC 1/SSAE 16/ISAE 3402

Tabitop's trusted third-party cloud partner(s) publishes a Service Organization Controls 1 (SOC 1), Type II report . The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402).

This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. This dual-standard report can meet a broad range of auditing requirements for U.S. and international auditing bodies.

The SOC 1 report audit attests that the Tabitop's third-party cloud partner(s) control objectives are appropriately designed and that the controls safeguarding customer data are operating effectively. Tabitop's trusted third-party partner(s) SOC 1 report includes all Tabitop's trusted third-party partner(s) data centers worldwide that support in-scope services.

SOC 2

In addition to the SOC 1 report, Tabitop's trusted third-party cloud partner(s) publishes a Service Organization Controls 2 (SOC 2), Type II report . Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles . These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as Tabitop's trusted third-party cloud partner(s). The Tabitop's trusted third-party cloud partner(s) SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security principle set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into Tabitop's trusted third-party cloud partner(s) security based on a defined industry standard and further demonstrates Tabitop's commitment to protecting customer data. The Tabitop's trusted third-party cloud partner(s) SOC 2 report includes all Tabitop's trusted third-party cloud partner(s) data centers worldwide that support in-scope

services.

SOC 3

Tabitop's trusted third-party cloud partner(s) publishes a Service Organization Controls 3 (SOC 3) report . The SOC 3 report is a publically-available summary of the Tabitop's trusted third-party cloud partner(s) SOC 2 report and provides the AICPA SysTrust Security Seal.

The report includes the external auditor's opinion of the operation of controls (based on the AICPA's Security Trust Principles included in the SOC 2 report), the assertion from Tabitop's trusted third-party cloud partner(s) management regarding the effectiveness of controls, and an overview of Tabitop's trusted third-party cloud partner(s) Infrastructure and Services. The Tabitop's trusted third-party cloud partner(s) SOC 3 report includes all Tabitop's trusted third-party cloud partner(s) data centers worldwide that support in-scope services. This is a great resource for customers to validate that Tabitop's trusted third-party cloud partner(s) has obtained external auditor assurance without going through the process to request a SOC 2 report.

PCI DSS Level 1

Tabitop's trusted third-party cloud partner(s) is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS). Customers can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. In February 2013, the PCI Security Standards Council released PCI DSS Cloud Computing Guidelines . These guidelines provide customers who are managing a cardholder data environment with considerations for maintaining PCI DSS controls in the cloud. Tabitop's trusted third-party cloud partner(s) has incorporated the PCI DSS Cloud Computing Guidelines into the Tabitop's trusted third-party cloud partner(s) PCI Compliance Package for customers. The Tabitop's trusted third-party cloud partner(s) PCI Compliance Package includes the Tabitop's trusted third-party cloud partner(s) PCI Attestation of Compliance (AoC), which shows that Tabitop's trusted third-party cloud partner(s) has been successfully validated against

standards applicable to a Level 1 service provider under PCI DSS Version 2.0, and the Tabitop's trusted third-party cloud partner(s) PCI Responsibility Summary, which explains how compliance responsibilities are shared between Tabitop's trusted third-party cloud partner(s) and our customers in the cloud. The Tabitop's trusted third-party cloud partner(s) PCI DSS Level 1 certification includes all Tabitop's trusted third-party cloud partner(s) data centers worldwide that support in-scope services.

ISO 27001

Tabitop's trusted third-party cloud partner(s) is ISO 27001 certified under the International Organization for Standardization (ISO) 27001 standard. ISO 27001 is a widely-adopted global security standard that outlines the requirements for information security management systems. It provides a systematic approach to managing company and customer information that's based on periodic risk assessments. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information.

Tabitop's trusted third-party cloud partner(s) has established a formal program to maintain the certification. This certification reinforces our commitment to providing transparency into our security controls and practices. The Tabitop's trusted third-party cloud partner(s) ISO 27001 certification includes all Tabitop's trusted third-party cloud partner(s) data centers worldwide that support in-scope services.

Cloud Security Alliance

In 2011, the Cloud Security Alliance (CSA) launched STAR , an initiative to encourage transparency of security practices within cloud providers. The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. Tabitop's trusted third-party cloud partner(s) is a CSA STAR registrant and has completed the Cloud Security Alliance (CSA) Consensus Assessments

Initiative Questionnaire (CAIQ). This CAIQ published by the CSA provides a way to reference and document what security controls exist in Tabitop's trusted third-party cloud partner(s)' Infrastructure as a Service offerings. The CAIQ provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.

Sharing the Security Responsibility

Because users are building virtual desktop PC instances within the Tabitop cloud infrastructure, the security responsibilities will be shared: Tabitop has secured the underlying infrastructure and each user is responsible for securing any and all desktops, software, and systems put on the infrastructure. This includes user's Tabitop virtual desktop PC instances and anything that is installed on them, any accounts that access the user instances, the security firewall software that allows outside access to your instances, etc.

Contacting Tabitop Security

The Tabitop Security Team encourages customer communication. Please feel free to contact us directly at security@tabitop.com.