TRACKVIA SECURITY OVERVIEW

GOVERNANCE
COMPLIANCE
RISK MANAGEMENT
TOOLS
PEOPLE
PROCESSES

TrackVia's customers rely on our service for many mission-critical applications, as well as for applications that have various compliance and regulatory obligations. At all times TrackVia considers the security, integrity and reliability of our customers' data to be our highest priority. In order to effectively meet our customers' needs, TrackVia's engineering and operations group has created a security, governance and risk management framework of policies, procedures and standards.

TrackVia's commitment to the security, integrity and reliability of our platform includes technology choices, certifications, policies and procedures, and customer-centric testing and update procedures. Highlighted in this document are the details of each of those areas.

Should you require information on any other specific security, integrity or reliability concerns, please contact your sales or support representative and we will be sure to address your questions.

DATA CENTER OPERATIONS

As a cloud-based solutions vendor, TrackVia delivers its enterprise-grade service via distributed third-party data center providers located primarily in the United States. TrackVia can also provide international-based operations should you have specific geographic requirements. The security processes, procedures, technologies and controls described in this section reflect both the internal security practices of TrackVia as well as those of the third-party data centers we utilize to deliver our service to customers.

Network security

TrackVia and our data center partners maintain extensive standards for ensuring network security at all times:

- *Network security is monitored 24/7 and automated alarms exist for any potential problem.*
- *TrackVia monitors industry-wide communications about new attacks and compromises, and immediately acts on identified vulnerabilities in any third-party component in place. Historically, TrackVia has implemented published updates within less than 24 hours. (See the section "Security monitoring, auditing and incident response" below for additional details.)*
- *A standard configuration for all components of our production environment exists and includes turning off non-critical or unused services, blocking all ports except those*

Rev. November 2016

specifically required, eliminating any unused standard logins, and configuring all used logins properly to require the appropriate authentication and encryption.

- *TrackVia has implemented two-factor authentication for access to any production environment by our 24/7 Operations team, and for making any changes to production environments.*

Redundancy and backups

TrackVia operates out of at least three geographically disparate data centers, protecting against a variety of natural disasters or data-center-wide outages. All data centers are fully active at all times, ensuring no delay in the event of a full data center failure.

Within each data center, TrackVia maintains redundancy at multiple tiers of our architecture. There are multiple application servers at all times to provide application functionality, and data is replicated across multiple database instances in real time, ensuring that multiple physical storage devices are fully up to date at all times to protect against any storage system failure.

Backups across all customer data and operational data occur on a daily basis and can be used to restore an account to a prior state upon customer request. All backup operations performed by TrackVia are encrypted using AES-256, and are encrypted in transit and at rest. Backups are automatically aged off and deleted per our published schedule, ensuring that no remnant data remains after any deletion you may undertake. Backups are securely transmitted and stored in yet another geographically separate data center, separate from the three or more active data centers.

DISASTER RECOVERY

TrackVia has implemented a comprehensive disaster recovery plan that allows for the possibility of the loss of an entire data center without impacting customer data or immediate, ongoing access to that data and associated application functionality.

Key elements of this disaster recovery plan include:

- *As a result of the active-active data center model described in the previous section, there is no delay or outage introduced as a result of the loss of a data center. All application functionality and data integrity remains in place across other active data centers. In addition, there is no opportunity for an incorrect configuration, version or other difference to exist, which typically can result from the use of a "standby" data center that might not be fully updated at all times.*

- *Each active data center has a certain amount of excess capacity at all times in order to take on additional traffic from a failed data center, and additional capacity can be activated in a window of approximately fifteen minutes as needed.*

- *TrackVia's 24/7 Operations team maintains full access and ability to manage production environments in the event of any outage affecting TrackVia's offices. Remote access is maintained with no degradation of security tools or policies.*

- *TrackVia's Customer Support team maintains full capabilities in the event of any outage affecting TrackVia's offices. All email, chat, telephone and other means of support can be remotely accessed as needed.*

Rev. November 2016

SECURITY FEATURES

The TrackVia platform contains several different features addressing the various dimensions of an enterprise-grade, secure platform. Several of those features are described in this section.

Encryption

TrackVia has implemented data encryption in several different ways. First, all access to TrackVia, whether via the Web application, mobile applications or API access is always fully encrypted in transit. All communications are encrypted via SSL at all times, including any email sent from the system (e.g., via the Notifications functionality), which is handled via TLS.

Second, TrackVia offers full at-rest encryption so your data is fully encrypted when stored within the TrackVia databases. In the highly unlikely event of a network breach or bypassing of multiple levels of application security, this means that your data will still be unreadable to an unauthorized party.

Third, as described above, all backup operations performed by TrackVia are encrypted using AES-256, and are encrypted in transit and at rest.

Authentication

All users accessing your TrackVia account are individually created and authorized by you, based on your administrative activities. At any time you have full visibility into your users, and can create users or deactivate users. Each user is required to have a password that meets certain strength requirements.

TrackVia has invested heavily in ensuring complete isolation between your account and any other. There is no cross-account functionality at all within the product, and account isolation is a key aspect tested in our recurring security audit (described below in the "Security monitoring, auditing, and incident response" section.) As an administrator of your own account, you have full visibility and control over all access to your applications and your data.

Finally, TrackVia can only access your account with your explicit permission and will only do so in order to provide support that you request. You may enable or disable this access at any time, and in fact, you must enable this access for TrackVia Support personnel to have any access at all to your account.

Roles and permissions

As an administrator, you have full control in creating the roles and permissions for each user. You can restrict access to any part of your data by creating the necessary roles and permissions within the platform, and assigning specific views, reports, filters and dashboards to the appropriate roles. By doing so, you retain full visibility and control, and can ensure that your security policies apply to any and all data stored within TrackVia.

Rev. November 2016

CERTIFICATIONS

Our data center partners have received numerous third-party certifications to ensure the security, integrity and reliability of your applications and data. Following are details about many of these certifications, some of which require specific implementation details and coordination with you to ensure compliance. Should you have any specific certification questions, please contact your sales or support representative.

Data Center Certifications

- ***PCI DSS Level 1***
- ***SOC 1 / ISAE 3402***
- ***SOC 2***
- ***SOC 3***
- ***ISO 9001***
- ***IRAP***
- ***FIPS 140-2***
- ***MPAA***
- ***HIPAA***
- ***FedRAMP (SM)***
- ***DoD CSM***
- ***DIACAP and FISMA***
- ***ISO 27001***
- ***MTCS Tier 3***
- ***ITAR***
- ***CSA***

HIPAA compliance

TrackVia offers a HIPAA-compliant option and can enter into a Business Associate Agreement (BAA) should it be required.

TrackVia has implemented technical and policy solutions around the Technical Safeguards, Physical Safeguards and Administrative Safeguards aspects of HIPAA's Security Rule. In addition, TrackVia complies with the Privacy Rule and Breach Notification Rule sections of HIPAA.

Further details on TrackVia's HIPAA-compliant solution are available through your sales or support representative.

Rev. November 2016

TRUSTe

TrackVia, Inc. has been awarded TRUSTe's Privacy Seal signifying that this privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's Program Requirements (http://www.truste.com/privacy-program-requirements/) including transparency, accountability and choice regarding the collection and use of your personal information.

The TRUSTe program does not cover information that may be collected through downloadable software. The TRUSTe program covers only information that is collected through this website, http://www.trackvia.com, and does not cover information that may be collected through our mobile applications or behind the log in on our website.

U.S. I EU Privacy Shield

TrackVia actively complies with the EU-U.S. Privacy Shield Framework, which was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables U.S.-based organizations to join the Privacy Shield Framework in order to benefit from the adequacy determination.

SECURITY MONITORING, AUDITING AND INCIDENT RESPONSE

Maintaining and monitoring the security of TrackVia's production operations is a critical aspect of our day-to-day operational management, as well as our long-term architectural planning, design and implementation. There are four key aspects of these security operations:

- *Identification*
- *Remediation of identified vulnerabilities*
- *Notification to customers in the event of a security incident*
- *Transparency*

Identification

TrackVia evaluates the security of our operational systems in multiple ways. At the highest level, TrackVia engages a third-party security audit on an annual basis. This audit consists of both penetration testing (active attempts by security-trained engineers designed to probe for weaknesses in system security and attempt to breach system security) and a vulnerability assessment (a review and classification of potential vulnerabilities by ease of attack or likelihood and risk level or impact.) TrackVia's security auditors test and report on the criticality and likelihood of potential attack vectors, provide details to TrackVia and conduct a subsequent retest after TrackVia has addressed any vulnerabilities.

The second level of security monitoring consists of both automated systems and manual procedures to monitor attempted accesses to the system (e.g., login successes and failures), any changes made to production systems, and reacting to published vulnerabilities (via mechanisms such as the Common Vulnerabilities and Exposures or CVE system maintained at https://cve.mitre.org/ and https://nvd.nist.gov/).

The third level of monitoring is conducted by TrackVia's data center partners, and includes active systems for Intrusion Detection Services, Intrusion Prevention Services and related network management.

Remediation

Remediation of any weaknesses or vulnerabilities identified in our third-party security audit is addressed at a high priority within our product development lifecycle. In our most recent security audit, no high or medium priority vulnerabilities remained at the conclusion of the audit (a total of three high and two medium priority items were initially identified and resolved prior to the conclusion of the audit).

TrackVia's 24/7 Operations team maintains the goal of fully patching production systems within 8-24 hours of a new vulnerability and has consistently met that goal. For any new vulnerability, TrackVia's Operations team evaluates the risk of the vulnerability and the risk of instability resulting from responding to the vulnerability (i.e., a potentially incomplete or erroneous initial fix), and will take appropriate action within that 8-24 hour period.

Finally, TrackVia is notified by our data center partners of any broader network-level potential vulnerabilities and coordinates to address issues immediately.

Notification

TrackVia has mechanisms in place to notify customers of any identified breach within 24 hours. In addition, TrackVia proactively works to keep customers informed of TrackVia's security stance and response to specific vulnerabilities. Direct communications to customers are made within 24 hours, and additional broad updates are also provided via our blog (e.g., http://www.trackvia.com/blog/company-news/trackvia-security-heartbleed-vulnerability and http://www.trackvia.com/blog/company-news/trackvia-engineering/trackvias-response-vulnerability-cve-2014-6271-aka-shellshock).

Rev. November 2016

Transparency

TrackVia is committed to proactively communicating any security incidents to our customers, as well as providing clear, public reports of the availability of our service. At any time the status of the TrackVia service can be reviewed at TrackVia's System Status page (http://www.trackvia.com/about-us-trackvia/trackvia-system-status/), which reports on the current operational status and historical availability of the service.

UPGRADE AND RELEASE PROCEDURES

TrackVia has an automated build and deploy process to ensure consistency and avoid human error. We deploy through testing and staging environments prior to production releases. We execute a suite of automated tests during any build or deploy. Most updates are zero-downtime and do not impact users. We also monitor security alerts and patch OS and supporting tools as appropriate, and system-level patches are handled in an automated manner across our entire infrastructure.

Typically updates occur at least weekly and are either transparent or provide a brief alert during a browser session to refresh and begin using the new version.

Nearly all releases are non-impacting to clients. Releases that require a system-wide maintenance window have historically been less than one per quarter, are done at low-usage times, and are done after providing a seven-day notification to customers. We have the ability to slow-roll releases to a subset of clients (for purposes such as "beta", "early look", as well as risk reduction.) We maintain full backward compatibility for all public API updates. Prior releases are kept in place for a minimum of 24 hours to provide for immediate rollback capabilities should it be required.

DATA OWNERSHIP AND EXPORT

TrackVia at no time has any ownership of your data in any way — your data always remains fully under your ownership in all legal manners, and fully under your control.

While TrackVia is very confident in the high-availability, highly redundant infrastructure in place to protect customer data against all variety of potential events, we also recognize that customers should always have access to mechanisms for exporting data from the TrackVia system. TrackVia provides several mechanisms in support of this requirement:

- *Customers have direct access to export capabilities for every table in any of their applications, allowing for an easy-to-use and easy-to-execute download of all data in a comma separated value (CSV) format that can be easily handled or imported into any other system. Access to this export capability for users within your account can be restricted by customers in their administrative role.*
- *Customers may request an export of large volumes of data to portable physical storage (USB stick, portable hard drive, etc.), which is provided directly to an authorized representative of the customer.*
- *Customers can consult with TrackVia's Customer Support team at any time to discuss a specific data export requirement.*

SECURITY POLICIES

TrackVia maintains policies around operational access to customer data. Access to production environments is limited to a very small number of people who manage the day-to-day operations of TrackVia's production environments. All access is individually assigned (no shared logins) and all access is logged and reviewed. Customer data is not used in any non-production environments for testing or any other purposes. As described above in the "Authentication" section, TrackVia's support personnel do not have access to any customer data except in cases where a customer has taken explicit action to grant that access in order to provide customer support. If granted, that access can be explicitly removed at any time by customers.

CONCLUSION

TrackVia recognizes that a strong commitment to the security, integrity and reliability of our platform and our customers' data is critical. This commitment exists at all levels of our operation, from the security reviews conducted as part of our ongoing development process to the day-to-day security monitoring and management in our 24/7 Operations team to the security controls provided within the application and around customer support access. TrackVia is committed to providing a highly reliable, highly available, and highly secure solution for your enterprise-grade and mission-critical application needs.

Rev. November 2016