Last Update: March 4, 2019

Purpose

We keep information security and data security at the top of our minds here at TrenDemon. We built our product with this in mind from the very beginning. Presented in this document are security standards that TrenDemon complies with as well as policies and procedures.

Scope and Applicability

This TrenDemon Information and Data Security Policy (*"IDSP"*) summarizes TrenDemon's handling of data and information which it collects in the course of conducting its business, including, management's role, training, confidentiality of client data, acceptable use of resources, and more (collectively, the *"Information Security Program"*). All TrenDemon staff must review this policy during on-boarding.

TrenDemon's Information and Data Security Policy relies on various procedures implemented throughout TrenDemon's operations, including specialized policies and procedures governing practices such as incident response process, audits, security, and backups. This IDSP is a summary of the Information Security Program, as more detailed policies and procedures are defined as standalone documents, and communicated separately to the appropriate audience on a confidential basis and are generally not shared to non-TrenDemon employees unless required by law or to improve TrenDemon's data handling and security practices (e.g., outside consulting firms or contractors subject to confidentiality obligations). To the extent this IDSP is shared with non-TrenDemon employees, such individuals or entities who receive this IDSP must keep this IDSP confidential unless disclosure is otherwise allowed by TrenDemon in writing. To the extent

this IDSP is disclosed to a non-TrenDemon employee (e.g., a TrenDemon customer), the recipient acknowledges that this IDSP does not create any warranties or covenants of any kind by TrenDemon unless agreed upon in a writing executed by the recipient and TrenDemon. TrenDemon may update this IDSP from time to time in its sole discretion.

The IDSP should be read in conjunction with TrenDemon's Privacy Policy (the "Privacy Policy").

Updates to this Policy

TrenDemonmakes routine updates to this Information and Data Security Policy and will always show the latest version with the date of the most recent update.

TrenDemon may also change its Privacy Policy on occasion.

From time to time, TrenDemon may agree to specific policies for specific customers. When these policies change, the changes will be handled through direct communication with the customer and the execution of a new document detailing the edits to the existing agreement.

Audience

These standards and policies apply to all TrenDemon employees, contractors, suppliers, customers, and all other users of TrenDemon information systems that support the operations and assets of TrenDemon.

Shared Responsibility

While TrenDemon makes every effort to fulfill our defined responsibilities, customers are ultimately responsible for the security of their data as per the TrenDemon's Terms of Service. Customers are responsible for maintaining the confidentiality of their Account login information and are fully responsible for all activities that occur under their Account. As customers, you agree to immediately notify TrenDemon of any unauthorized use, or suspected unauthorized use of your Account or any other breach of security. If any breach is suspected, contact support@trendemon.com immediately.

Background

TrenDemon has developed standards and policies outlining necessary responsibilities to ensure the confidentiality, integrity, and availability of TrenDemon's information and information systems. All data is hosted and stored securely in Amazon Web Services data centers which fulfill the security, privacy, compliance, and risk management requirements as defined in the Cloud Security Alliance (CSA).

Roles and Responsibilities

This section provides roles and responsibilities for TrenDemon employees who have access to confidential data, with a responsibility for protecting the information and information systems.

Only authorized TrenDemon personnel can administer systems or perform security management and operational functions. Authorization for and implementation of changes are segregated responsibilities wherever appropriate to the organization.

Data Classification

TrenDemon collects, aggregates, processes and handles a variety of types of information in connection with its business. For purposes of the Information and Data Security Policy, TrenDemon categorizes such information as follows:

Public

Public data is information that may be disclosed to any person regardless of their affiliation with TrenDemon, i.e., data that does not require any level of protection from disclosure. Public data may be shared with a broad audience both within and outside TrebDemon and no steps need be taken to prevent its distribution. Examples of public data include: press releases, news articles about TrenDemon or its customers, information general available on the Internet which is not subject to any contractual (e.g., terms of service) or legal (e.g., copyright) restrictions.

Internal

Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data generally should not be disclosed outside of TrenDemon without the permission of the person or group that created the data. It is the responsibility of the data owner to designate information as internal or “for TrenDemon eyes only” where appropriate, however, TrenDemon employees are trained to identify data which by its nature should be classified as internal data. Examples of Internal data include: internal memos, correspondence, and corporate meeting minutes, internal e-mail correspondence, contact lists that contain information that is not publicly available, and procedural documentation that should remain internal.

Confidential

Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or the business who created and/or disclosed such confidential information. This classification also includes data that TrenDemon is required to keep confidential, either by law or under a confidentiality agreement with an individual or entity unaffiliated with TrenDemon, such as a customer. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes or as otherwise allowed by the Privacy Policy, and should be protected both when it is in use and when it is being stored or transported.

It is the responsibility of the person using the data and/or disclosure to designate information as “confidential” where appropriate. Individuals and departments that create or circulate confidential data should clearly designate the data by clearly marking both hard copies and electronic version of documents as confidential. Those who receive data marked as confidential should take appropriate steps to protect it.

Any unauthorized disclosure or loss of confidential data must be reported to TrenDemon’s Head of Customer Success. Such executive, working with TrenDemon’s IT team, will determine if confidential information was indeed disclosed. If confidential information was improperly disclosed, TrenDemon will notify affected parties as required by law, contract and/or in accordance with this TrenDemon’s Information and Data Security Policy.

TrenDemon classifies two categories of confidential data: confidential customer data and confidential PII data.

Examples of confidential customer data include:

- All data collected by TrenDemon on behalf of the customer, except for confidential PII data. This includes, but is not limited to, web page URLs that visitors access on the Customer website, the web page referral URL, The visitor's browser user-agent information. the time of the page view, indication of specific user events, such as page reads and interactions with TrenDemon's personalization units
- Information that is the subject of a confidentiality agreement

Examples of confidential PII data include:

- Personally identifiable information entrusted to our care specifically email address, IP address, and cookie information.

Data Usage

TrenDemon collects information from our visitors and customers who provide it explicitly (like name, email, billing information, address, etc.) or implicitly (like web browser type and language, IP address, marketing source, etc.). The use of user data collected through our services shall be limited to the purpose of providing the services requested by the Customer.

TrenDemon does not sell personal information to third parties. TrenDemon does not use any third party personal information contained in our Customers' customer data in ad targeting. Customers' customer data means any and all information and content that a user submits to, or is collected through the TrenDemon javascript, or other online services which you connect to TrenDemon, or your business website.

Client Data Management

Access to client data is restricted to legitimate business use only.

TrenDemon may publish anonymized and aggregated information from Customers' customer data for marketing or any other lawful purpose, with the option for customer opt-out.

TrenDemon ensures secure transport and storage of data. Any and all transport of confidential customer data data is via secure connection (HTTPS). TrenDemon maintains logical separation of user data between customers. During the system design and development process the same stringent data management is used, and pre-production systems are deployed in identically secure environments as production.

Unless otherwise stated, confidential customer data is deleted from storage mediums within 90 days after the relationship between the client and TrenDemon ends.

Access Control

Restricting Access

All application and database access requests should be granted by the Head of Engineering (currently VP R&D). Access is granted based on legitimate business need based on a need-to-know principle. Access is revoked immediately upon termination.

User Access Review

Database access and permissions are reviewed on an annual basis. The TrenDemon Head of Engineering & Head of Customer Success must review accounts of Users who can access confidential data and information systems and ensure that their ability to access and level of access is appropriate.

Shared Accounts

Shared accounts is strictly prohibited under any circumstance. Unique user IDs are created for each employee. TrenDemon does not allow employees to access confidential data using a shared account, including but not limited to, access to the application and logging into the database.

Remote Access

This policy applies to remote access connections used to do work on behalf of TrenDemon, including accessing code repositories and production databases, excluding email. Remote access is disabled by default, including for Authorized Users. Permission must be explicitly approved by the Head of Engineering. When accessing the TrenDemon network from outside of the office network, Authorized Users are responsible for preventing access to any TrenDemon resources or data by non-Authorized Users. Authorized Users shall protect their login and password, even from family members. While remotely connecting to TrenDemon's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control. All hosts that are connected to TrenDemon internal networks via remote access technologies must use the most up-to-date anti-virus software.

Performance of illegal activities through the TrenDemon network by any User (Authorized or otherwise) is prohibited.

Software Development Lifecycle

Purpose

TrenDemon has an established and formal Software Development Lifecycle Policy (*"SDLC"*) and supporting procedures. The policy and procedures are designed to provide the TrenDemon Product and Development teams with a documented and formalized SDLC that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of TrenDemon's system resources. Below is a brief summary of the policy.

Scope

This policy and supporting procedures encompasses all system resources that are owned, operated, maintained, and controlled by TrenDemon and all other system resources, both internally and externally, that interact with these systems.

- Internal system resources are those owned, operated, maintained, and controlled by TrenDemon and include all network devices (firewalls, routers), workstations, and other system resources deemed in scope.
- External system resources are those owned, operated, maintained, and controlled by any entity other than TrenDemon like servers (both physical and virtual servers, along with the operating systems and applications that reside on them).

Change Management

Key processes and security checks in TrenDemon's production environment are documented. All changes to the production environment (network, systems, platform, application, configuration,

including physical changes such as equipment moves) are tracked and implemented by a dedicated team. All deployments into production or change to the production environment (network, systems, platform, application, configuration, etc.) must be submitted to, reviewed and approved by the relevant stakeholders within TrenDemon who are familiar with the Information and Data Security Policy.

Both scheduled and emergency changes are tested in separate environments, reviewed and approved by product and development before deployment to the production environment.

Testing

Manual vulnerability testing is performed during the development process. TrenDemon uses documented procedures to build and configure systems, platforms and applications to minimize security risks. TrenDemon deploys security fixes to the extent a vulnerability is identified.

Application Hardening

All TrenDemon systems run in secure datacenters, that are managed and maintained by expert 3rd parties (Amazon Web Services). These 3rd parties provide all of our network level services, including load balancers, and network security. In addition, they provide services for intrusion detection, and DDOS.

Operations Security

TrenDemon's IT and software development teams use prevailing industry standards to manage the day-to-day security of its internal systems which touch upon the data and information handled by TrenDemon, such as default deny rules for firewalls, intrusion detection systems and patch management.

Risk Assessment

TrenDemon has practices in place to assist management in identifying and managing potential internal and external risks that could negatively affect the organization's critical business processes and our ability to provide reliable services to our clients. The approach is to understand the existing system and environment and identify risks through analysis of the information and data being collected. These practices are used to identify significant risks for the organization, initiate the identification and/or implementation of appropriate risk mitigation measures, and assist management in monitoring risk and remediation activities.

Asset Management

Personal computers and laptops are provided to all TrenDemon employees to perform work-related tasks. TrenDemon does not supply employees with mobile devices nor does it support a Bring Your Own Device (BYOD) policy. TrenDemon maintains a centralized asset management platform to keep and administer an up-to-date inventory of TrenDemon's assets.

Electronics Policy

All documents, apparatus, equipment, electronic media, and other physical property is the sole property of TrenDemon. All internal or confidential data must be protected at all times from anyone who may pass by including other employees, cleaners, and office visitors. All documents, materials and property will be returned to TrenDemon when requested. All other unauthorized equipment is not allowed on the office network.

Removable Media Devices

TrenDemon prohibits copying client and confidential data on a removable media device, including flash drives, hard drives, tapes or other media. Removable media devices may be used for legitimate business purposes handling internal data such as presentations and slides, as long as no customer data is included. All personnel who handle storage media must comply with the Information Data and Security Policy.

Anti-Virus/Anti-Malware Protection

All TrenDemon workstations have antivirus software deployed with automatic update, and are scanned per policy.

All production services with any internet facing endpoint has anti-virus and anti-malware software installed and are scanned regularly.

Incident Management

TrenDemon has in place an incident management process (“IMP”) to address data breach and security events related to its products and services in an efficient and timely manner. Incidents can be identified by Users, customers, suppliers, or TrenDemon employees. An “incident” is a potential security or data breach which could include, but is not limited to: phishing, hacking, software piracy, cyber stalking, extortion, or threats. In certain cases (e.g., as required by applicable law and/or the agreement between TrenDemon and the affected customer), TrenDemon will notify client contacts assigned to the account as soon as possible after confirming them as being affected by a security or data breach. In compliance with the EU General Data Protection Regulation (GDPR), TrenDemon will also notify supervisory authority within 72 hours of becoming aware of it unless the breach is unlikely to pose a risk to the rights and freedoms of

natural persons. TrenDemon will also inform the data subject of the breach without undue delay unless the breach is unlikely to pose a risk to the rights and freedoms of those data subjects.

Monitoring

Application Monitoring

All TrenDemon applications are monitored for both system and application level events.

Backup System Configurations

TrenDemon leverages Amazon Web Services features, to ensure that data is replicated transparently to our backup datacenter, in event of datacenter loss.

Business Continuity/Disaster Recovery (BC/DR) Plan

Purpose

This purpose of the Business Continuity and Disaster Recovery Plan is to prepare TrenDemon in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. All TrenDemon sites are expected to implement preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs.

The plan identifies vulnerabilities and recommends necessary measures to prevent extended voice communications service outages. The scope of this plan is focused on localized disasters such as fires, floods, and other localized natural or man-made disasters, not national disasters such as nuclear war which are beyond the scope of this plan.

Below is a summary of the plan.

Background Information

TrenDemon's core product is a software-as-a-service in which all data is hosted in Amazon Web Services datacenters located in Virgina US. TrenDemon headquarters in Israel, does not have any datacenters or servers on-site.

In the event of interruption to use of TrenDemon premises, TrenDemon services should remain unaffected. Critical work from Success Managers and Development personnel can be effectively be conducted remotely while interim quarters are found and prepped. We anticipate some delay in responsiveness, during this time.

In the event of a datacenter outage, TrenDemon personnel will be unaffected, but there will be some level of interruption or delay in the delivery of TrenDemon services. In the worst case of a datacenter loss, TrenDemon will fail over to our backup datacenter. Note that there will be no loss of data from the outage, simply large delays in processing and delivery.

Employee Security

Confidentiality and security is a serious concern for our clients and TrenDemon employees are required to sign agreements which require the employees to keep client information confidential. Acknowledgement of the employee code of conduct (employee handbook) is required upon hire and each time updates are made. Topics covered include employee benefits, travel policy, anti-bribery/anti-corruption, privacy, physical property and incident reporting.

General information security training is provided to all new employees and repeated annually thereafter. Development and Product and IT staff receive training specific to product development, deployment and management of secure applications. Additional security training is also provided to employees who handle client data.

Violation of TrenDemon's security policies can result in employee discipline, including termination. TrenDemon's Human Resources department manages a formal termination process, which includes notification of IT, return of computers, and disabling of passwords. The exit interview reminds ex-employees of their remaining employment restriction and contractual obligations.

Supplier Relationships

TrenDemon may use contractors for development, infrastructure management, testing and other legitimate processes. Some contractors may work under the direct supervision of TrenDemon employees and may have access to client data in accordance with contract terms as necessary for TrenDemon to conduct its business.

Generally, TrenDemon doesn't give suppliers direct access to client data or network/equipment management responsibility. TrenDemon uses exclusively established and reputable third party suppliers with respect to its IT and data handling systems, such as Amazon (for cloud infrastructure) and Google (for e-mail hosting).