DATA SECURITY POLICY

Organizational Controls

Solar Oil Enterprises Limited (the "Company") personnel are expected to be competent, thorough, helpful, and courteous stewards of customer information that is stored on the Company's products and in the Company's data centers. The Company has established a number of measures to ensure that customers and their data are treated properly.

Privacy and Control Mechanisms

The Company only uses the information provided by our customers to deliver the products and services purchased. All customer data is managed in compliance with our Privacy Policy. In addition, some products and all US Data Centers are audited to provide an independent validation of our policies and procedures around securing customer data.

The Company complies with any portion of HIPAA or the HITECH Act that are directly applicable to the Company. In particular, the Company Platform safeguards replicated data in such a way as to satisfy HIPAA's Security Rule. Customers wishing to establish a Business Associate relationship with the Company per 45 CFR 164.502(e) and 164.504(e) should request a Business Associate Agreement from the Company. The Business Associate Agreement defines commitments that the Company will make to maintain HIPAA and HITECH compliance as required

Company Employees

All employees are required to accept and acknowledge in writing the Company's policies for nondisclosure and protection of the Company and third-party confidential information, including acceptable use of confidential information. In the course of assisting customers with their technology solutions, the Company support technicians understand that they may come into contact with customer communications and/or customer data and they must keep this information confidential.

Training

Technicians who support the Company products are prepared in a variety of ways. New tier 1 technicians receive class time training with tier 2 technicians and the support management team. New support technicians also spend a period of time as an understudy to an established technician for each product in which they intend to become certified. Product knowledge is tested and established through formal online training and all technicians are expected to meet a pre-defined standard before supporting customers directly.

All Company support technicians receive ongoing training in product-specific training sessions.

When an employee or contractor leaves the Company, a formal process is in place to immediately revoke physical and network access to the Company's facilities and resources.

Architecture and Infrastructure Security

Storage Facility Standards

The Company leases space in a number of data centers worldwide. Each Company data center is equipped with the following:

- Controlled access systems requiring key-card authentication
- Video-monitored access points
- Intrusion alarms
- Locking cabinets
- Climate control systems
- Waterless fire-suppressant systems
- Redundant power (generator backup, UPS, no single point of failure)
- Redundant Internet connectivity
- ISO and/or SOC II certified

Data Location

Knowing the geographic location of their data is important for customers operating in regulated industries or in countries with data protection laws. The Company understands that some customers must maintain their data in a specific geographic location, such as within the European Union or within countries that are members of the Asia-Pacific Economic Cooperation (APEC) forum.

To that end, the Company maintains a network of Platform-scale data centers by geographic location around the globe, and verifies that each meets defined security requirements. However, not all Company products are deployed in all regions. To determine where data for a particular Company product is stored, please refer to the product-specific security document.

Redundancy

Data in the Company Platform is stored in a proprietary storage system developed and managed by the Company. This system maintains two copies of customer data to provide redundancy. In the United States, the two copies are stored in separate data center locations. Outside of the United States, the two copies are stored within the same location on separate storage systems.

Platform Security

The Company uses a defense-in-depth strategy and proprietary hardened software and operating systems to protect data and services. The Company conducts regular inspections to ensure the security of its systems.

Data Privacy

1. Your Data

Data stored in the Company Platform is our customers' data and we protect their right to make decisions about that data and we are transparent about what happens to that data. With the Company Platform, you are the owner of your customer data.

Customer data is defined as all data, including text, sound, video, or image files and software, that you provide to the Company, or is provided on your behalf.

The Company will use your customer data only to provide the services we have agreed upon, and for purposes that are compatible with providing those services.

You can access your customer data at any time and for any reason without assistance from the Company. We restrict access to it to the Company personnel and subcontractors. We provide simple, transparent data-use policies.

We do not use customer data for advertising

Except as set forth below, the Company does not share customer data with our advertiser-supported services, nor do we mine it for marketing or advertising.

In addition to providing the service and day-to-day operations, the Company may use your data for the following:

- Troubleshooting aimed at preventing, detecting, and repairing problems affecting the operation of services
- Ongoing improvement of features, such as those that improve the reliability of our services, or involve the detection of, and protection against, threats to the services or customer data (such as malware or spam)
- Providing personalized customer experiences
- Contacting you about new products and services

Furthermore, the Company Platform uses systems that are kept logically separate from internal systems run by the Company.

We use logical isolation to segregate each customer's data from that of others

The Company Platform services are multi-tenant services, meaning that your data, deployments, and virtual machines may be stored on the same physical hardware as that of other customers. When data from many customers is stored at a shared physical location, the Company logically segregates storage and processing for different customers through specialized technology engineered specifically for that purpose.

The Company takes strong measures to protect customer data from inappropriate use or loss and to prevent customers from gaining access to one another's data.

We provide simple, transparent data-use policies and get independent audits

The Company provides you with details of our data protection policies and practices in clear, straightforward language in the Privacy Policy.

Our subcontractors are contractually obligated to meet our privacy requirements

The Company may hire other companies to provide limited services, such as data colocation services. We provide customer data as required to deliver the services we have retained them to provide. Subcontractors are prohibited from using customer data for any other purpose, and they are required to maintain the confidentiality of our customers' information.

- Subcontractors who handle customer data in the Company Platform services must enter into additional agreements with the Company that subject them to data protection terms.
- Subcontractors who handle the Company Platform customer data in their own facilities are required to set up and follow privacy standards equivalent to our own.

Control of your Data

You control access to your customer data

Access by Company personnel.

The Company's personnel are granted access only when necessary under management oversight. The Company's personnel will use customer data only for purposes compatible with providing you the services, which can include customer support and troubleshooting services.

Access by subcontractors.

The Company may hire other companies to provide limited services. Subcontractors can access customer data only to deliver the services we have hired them to provide. Subcontractors are prohibited from using customer data for any other purpose, and are required to maintain the confidentiality of our customers' information.

Limits to access.

The operational processes and controls that govern access to and use of customer data in the Company Platform are regularly verified. The Company regularly performs sample audits to attest that access is only for legitimate business purposes. Strong controls and authentication help limit access to customer data to authorized personnel only. When access is granted, whether to the Company personnel or our subcontractors, it is carefully controlled and logged, and revoked as soon as it is no longer needed.

Government and law enforcement requests.

The Company imposes carefully defined requirements around government and law enforcement requests for customer data. We will not disclose data hosted in the Company Platform to a government agency except as you direct or where required by law. When we receive a government or law enforcement request for customer data, we attempt to redirect the third-party to obtain the requested data from our customer.

You control your customer data if you leave the service

The Company follows strict standards and specific processes for removing customer data from all systems under our control.

Data portability

You can retrieve a copy of your customer data at any time and for any reason without any assistance or notification required from the Company.

Data retention

- If you, the customer, terminate your subscription or it expires (except for free trials), the Company will store your customer data in a limited-function account for 30 days (the retention period) to give you time to export the data or renew your subscription. During this period, the Company provides multiple notices, so you will be amply forewarned of the upcoming deletion of data.
- After this 30-day retention period, the Company will disable the account and may delete all customer data at its discretion, including any cached or backup copies.

In the multitenant environments of the Company Platform services, we take careful measures to logically separate customer data to help prevent one customer's data from leaking into the data of another customer, as well as to help block any customer from accessing another customer's deleted data.

Data deletion on physical storage devices

- When a disk drive used for storage in the Company Platform suffers a hardware failure, it is securely erased or destroyed before the Company returns it to the manufacturer for replacement or repair. All of the data on the drive is completely overwritten to ensure that the data cannot be recovered by any means.

You have options to control the security of your customer data

The Company Platform uses encryption to safeguard your data and help you maintain control over it.

When customer data moves over a network, the Company Platform uses industry- standard secure transport protocols between user devices and Company data centers, as well as within the data centers themselves.

The Company Platform uses industry-standard encryption for data at rest in transit.

How we respond to government requests

When governments or law enforcement make a lawful request for customer data from the Company, we are committed to transparency and limit what we disclose. Because the Company believes that customers should control their own data, we will not disclose data hosted in the Company Platform to a government or law enforcement agency except as you direct or where required by law.

We do not offer direct access to customer data.

We believe that you should control your own data. The Company does not give any third-party (including law enforcement, other government entity, or civil litigant) direct or unfettered access to customer data except as you direct, or as required by law.

We redirect law enforcement and other third-party requests to the customer.

When we receive a government or law enforcement request for customer data, we always attempt to redirect the third third-party to obtain the requested data from our customer.

For valid requests that we are not able to redirect to the customer, we disclose information only when we are legally compelled to do so, and we always make sure that we provide only the data specified in the legal order.

In either case, requests may require the release of the customer's basic contact information.

We do not give access to platform encryption keys.

We do not provide any government with our encryption keys or the ability to break our encryption.

Acceptable Use and Conduct

All users must be registered to access the Company Platform. Individual users must register using their name, and entity users must register under the legal name of their entity. You will be solely responsible and liable for any activity that occurs under your account.

You are solely responsible for the legality and appropriateness of your customer data uploaded or otherwise placed into the Company Platform.

The Company may immediately and without prior notice to You, remove any content or data, or suspend or cancel accounts if it becomes aware of any misuse or illegal actions associated with an account or user.

When using the Company Platform, you must not use the services to do any of the following things:

- Copy or upload files or information unless you have a legal right to the files or information;
- Probe, scan, or test the vulnerability of any system, or attempt to circumvent any security or authentication measures;
- Access, tamper with, or use non-public areas of the Company Platform. or attempt to access or search the Company Platform through non-public interfaces;
- Attempt to disrupt any user or network by sending a virus, malware, overloading, flooding, spamming, or mail-bombing, or otherwise interfere with the use of other users;
- Send unsolicited communications, promotions, advertisements, or spam;
- Attempt to access another user's account;
- Send altered, deceptive, or false source-identifying information, including "spoofing" or "phishing";
- Publish anything that is fraudulent, misleading, or infringes on another's rights;
- Misrepresent yourself or affiliation with an entity; or
- Publish or share materials that are offensive, defamatory, or unlawful.

Export Restrictions

The Company Platform services may be controlled for export purposes. You must comply with all United States export laws and regulations. You assume sole responsibility for any required export approval and/or licenses and all related costs and for the violation of any United States export law or regulation. If you are located in a country subject to embargo by the United States government, you are not entitled to use the Company Platform services.

Updated: November, 2020