Trust Systems Software (UK) (t/a TRUSTOPIA)
(Revision December 2018)

This TRUSTOPIA Security, Privacy And Architecture Standard (“TSPA”) forms part of the Master Subscription Agreement and or other written or electronic agreement(s) between TRUSTOPIA and YOU (the Customer) for the purchase of online and/or professional services (including associated TRUSTOPIA offline or mobile components) from TRUSTOPIA (identified either as “Services” or otherwise in the applicable agreement, and hereinafter collectively defined as “Services”) (the “Agreement”) to reflect the parties’ agreement with regard to the Processing of Personal Data, in accordance with the requirements of applicable Data Protection Laws and Regulations.

By signing the Master Subscription Agreement & Data Processing Addendum, a Customer acknowledges the existence of the TSPA and its specific terms on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorised Affiliates, if and to the extent TRUSTOPIA processes Personal Data for which such Authorised Affiliates qualify as the Controller.

For the purposes of this TSPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorised Affiliates. All capitalised terms not defined herein shall have the meaning set forth in the Agreement.

TRUSTOPIA’s Corporate Trust Commitment

TRUSTOPIA is committed to achieving and maintaining the trust of its customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across its suite of services, including data submitted by customers to our services (“Customer Data”).

Services Covered

This documentation describes the architecture of, the security and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to TRUSTOPIA services.

Some of the elements described in this documentation, such as log retention, back-ups, disaster recovery and return and deletion of data, do not apply to the temporary developer testing environments and demonstration environment branded Sandbox. Use of any TRUSTOPIA service is subject to this documentation.

Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organisation IDs" and allows the use of customer and user role-based access privileges.

Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production (e.g. Sandbox).
For customers who elect to use TRUSTOPIA’s Process-As-A-Service: the specific infrastructure service used to host a customer’s user data is Amazon Web Services which means that the underlying physical infrastructure on which Customer Data is stored is that of a public cloud provider for what is commonly referred to as Infrastructure as a Service.

**TRUSTOPIA Infrastructure**

TRUSTOPIA uses Amazon Web Services (AWS) Cloud Servers to host its platform and follows Amazon’s best practices to ensure it provides the highest availability while putting the strongest possible safeguards in place regarding customer privacy and segregation.

TRUSTOPIA owns or controls access to the infrastructure that TRUSTOPIA uses to host Customer Data submitted to TRUSTOPIA services. For information on limited infrastructure functions provided by third parties, see below in “Third-Party Infrastructure.”

Each instance of the TRUSTOPIA Services utilises various servers and other elements to make them run. Each primary instance in the AWS environment has a secondary mirror copy available at all times.

TRUSTOPIA hosts and runs its platform as a service via Amazon Web Services servers in the UK. The instance a client organisation may be using is indicated in the browser’s address bar.

A visual representation of TRUSTOPIA’s infrastructure architecture can be seen here:
Control of Processing

TRUSTOPIA has implemented procedures designed to ensure that customer data is processed only as instructed by the customer, throughout the entire chain of processing activities by TRUSTOPIA and its sub-processors.

In particular, TRUSTOPIA and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities.

Compliance with such obligations as well as the technical and organisational data security measures implemented by TRUSTOPIA and its sub-processors are subject to regular audits.

Third-Party Architecture

Currently, TRUSTOPIA uses Amazon Web Services exclusively for the hosting and delivery of its service as well as storage of data.

Audits and Certifications

The compliance certifications described herein apply to the Services that run on infrastructure hosted by TRUSTOPIA or managed by it:

- **Binding Corporate Rules (BCR) for Processors**: customer data submitted to TRUSTOPIA services is within the scope of the TRUSTOPIA BCR for Processors as set out in its Data Processing Addendum. The most current version of the TRUSTOPIA Data Processing Addendum is available on TRUSTOPIA’s website, currently located at [www.TRUSTOPIA.com](http://www.TRUSTOPIA.com)

Public Cloud Infrastructure is currently not within the scope of the above certifications because the deployment of the services on public cloud infrastructure has not yet been specifically included in external testing related to such certifications.

TRUSTOPIA’s public cloud vendor partner – Amazon Web Services (“AWS”) - maintains a robust set of certifications; information about security and privacy-related audits and certifications received by Amazon Web Services, Inc. (“AWS”) including information on their ISO 27001 certification and Service Organisation Control (SOC) reports, which are available from the AWS Security Website and the AWS Compliance Website.

ISO 27001

The ISO/IEC 27001:2013 certification for AWS covers the AWS security management process over a specified scope of services and data centres. Whilst TRUSTOPIA is not automatically certified by association; the decision to build out TRUSTOPIA infrastructure within the AWS cloud was made to also aid us as TRUSTOPIA pursues its own ISO/IEC 27001:2013 certification. It has been acknowledged that placing TRUSTOPIA’s infrastructure within the AWS cloud should make it easier to be certified.

A copy of the AWS certification can be viewed by following this URL: ISO/IEC 27001:2013
Security Controls

Access to the AWS console is handled with a tiered user permission structure taking advantage of AWS Identity and Access Management (IAM). The root access level is not used other than for initial configuration.

IAM policies are configured for Senior Developers and Junior Developers restricting privileges for junior to read only until such time as they are considered sufficiently competent and trusted to have their permissions increased. Senior Developers have enhanced permissions but are not permitted to delete content without requesting enhanced privileges to do so. Such privileges are issued on a request only basis following a written justified action request.

Access to TRUSTOPIA servers is controlled by public–key cryptography to encrypt and decrypt login information. Public–key cryptography uses a public key to encrypt a unique password and the recipient uses the private key to decrypt the data. The public and private keys are known as a key pair. The TRUSTOPIA private keys are held in an AES-256bit encrypted vault and only accessed when required by authorised parties†.

Once a TRUSTOPIA server has been configured the private key is not used again. The public keys belonging to the senior development team with explicit permission to access the server are added to the server ensuring that only their machines may access the server. This restricts access to a limited number of people and reduces the risk of unauthorised access due to a private key being intercepted.

Access to the RDS database is limited because it is only accessible via the EC2 instance to which it is associated and this means that it can only be accessed by the limited number of individuals with access to the EC2 as described above. In addition, the user would also need access to the MySQL password and this is only made available where a justifiable reason exists and permission must be sought from a senior member of the TRUSTOPIA management team.

The restrictions placed at this level are such that the management team must make a decision, confirm that the individual has been suitably checked for such access, and a grant of a window during which access may be obtained will be issued. Access to the password is shared within the encrypted vault and a developer is neither permitted nor able to retain a copy. Once the access window has expired, access to the password within the vault is revoked.

The TRUSTOPIA platform has been designed to satisfy the requirements of our most security-sensitive customers.

† This is the same encryption used by the US government for ‘top secret’ information and would take 149 trillion years to ‘crack’ only one entry encrypted with AES-256.
Security, Privacy, Architecture & Support

Security Procedures, Policies and Logging

TRUSTOPIA Services are operated in accordance with the following procedures to enhance security:

- User passwords are stored using a one-way salted hash.
- User access log entries are maintained, containing date, time, User ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
- If there is suspicion of inappropriate access, TRUSTOPIA can provide customers log entry records to assist in forensic analysis when available. This service is provided to customers on a time and materials basis.
- Datacenter physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- User Logs will be kept by TRUSTOPIA for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged.
- Certain administrative changes to the TRUSTOPIA Services (such as password change events) are tracked and are available for viewing by a customer’s system administrator on request.
- TRUSTOPIA personnel will not set a defined password for a user. Passwords are set to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

TRUSTOPIA Mobile Device Applications

TRUSTOPIA’s credentials for Google Play and iTunes Connect are held in an AES-256bit encrypted vault.

iOS

TRUSTOPIA is currently designed to work on iOS 10 and above. The TRUSTOPIA platform supports the current version of iOS along with the previous version by design so whilst at present, iOS 10 and iOS 11 are supported; once the updates are completed for iOS 12 (due October 2018) the minimum supported version will increase to iOS 11.

iOS versions of the application are currently optimised for mobile phone devices with tablet device optimisation in development. By design the latest security offerings are always available to TRUSTOPIA mobile app users.

EU & UK Data protection regulations are directly adhered to with TRUSTOPIA mobile app use in that no data whatsoever is stored on a mobile device is used to capture identity and or sensitive PII.
Android

The TRUSTOPIX Android mobile app is in development presently. The minimum Android version it will support will be 6.0 Marshmallow and above. Whilst currently there is an OS dating back to October 2015 that is officially unsupported; TRUSTOPIX recognises there are still a large number of users with devices running this generation of Android software. TRUSTOPIX believes it is important to try and balance device security vs user base and this is a compromise that TRUSTOPIX have decided to support.

<table>
<thead>
<tr>
<th>Code name</th>
<th>Version number</th>
<th>Linux kernel version</th>
<th>Initial release date</th>
<th>API level</th>
</tr>
</thead>
<tbody>
<tr>
<td>(No codename)</td>
<td>1.0</td>
<td>?</td>
<td>September 23, 2008</td>
<td>1</td>
</tr>
<tr>
<td>Petit Four</td>
<td>1.1</td>
<td>2.6</td>
<td>February 9, 2009</td>
<td>2</td>
</tr>
<tr>
<td>Cupcake</td>
<td>1.5</td>
<td>2.6.27</td>
<td>April 27, 2009</td>
<td>3</td>
</tr>
<tr>
<td>Donut</td>
<td>1.6</td>
<td>2.6.29</td>
<td>September 15, 2009</td>
<td>4</td>
</tr>
<tr>
<td>Eclair</td>
<td>2.0 – 2.1</td>
<td>2.6.20</td>
<td>October 26, 2009</td>
<td>5 – 7</td>
</tr>
<tr>
<td>Froyo</td>
<td>2.2 – 2.2.3</td>
<td>2.6.32</td>
<td>May 20, 2010</td>
<td>8</td>
</tr>
<tr>
<td>Gingerbread</td>
<td>2.3 – 2.3.7</td>
<td>2.6.35</td>
<td>December 6, 2010</td>
<td>9 – 10</td>
</tr>
<tr>
<td>Honeycomb</td>
<td>3.0 – 3.2.6</td>
<td>2.6.36</td>
<td>February 22, 2011</td>
<td>11 – 13</td>
</tr>
<tr>
<td>Ice Cream Sandwich</td>
<td>4.0 – 4.0.4</td>
<td>3.0.1</td>
<td>October 18, 2011</td>
<td>14 – 15</td>
</tr>
<tr>
<td>Jelly Bean</td>
<td>4.1 – 4.3.1</td>
<td>3.0.31 to 3.4.39</td>
<td>July 9, 2012</td>
<td>16 – 18</td>
</tr>
<tr>
<td>KitKat</td>
<td>4.4 – 4.4.4</td>
<td>3.10</td>
<td>October 31, 2013</td>
<td>19 – 20</td>
</tr>
<tr>
<td>Lollipop</td>
<td>5.0 – 5.1.1</td>
<td>3.16</td>
<td>November 12, 2014</td>
<td>21 – 22[13]</td>
</tr>
<tr>
<td>Marshmallow</td>
<td>6.0 – 6.0.1</td>
<td>3.18</td>
<td>October 5, 2015</td>
<td>23</td>
</tr>
<tr>
<td>Nougat</td>
<td>7.0 – 7.1.2</td>
<td>4.4</td>
<td>August 22, 2016</td>
<td>24 – 25</td>
</tr>
<tr>
<td>Oreo</td>
<td>8.0 – 8.1</td>
<td>4.10</td>
<td>August 21, 2017</td>
<td>26 – 27</td>
</tr>
<tr>
<td>Pie</td>
<td>9.0</td>
<td>4.4.107, 4.9.84, and 4.14.42</td>
<td>August 6, 2018</td>
<td>28</td>
</tr>
</tbody>
</table>

Legend: Old version | Older version, still supported | Latest version
Intrusion Detection

TRUSTOPIA, or an authorised third party, monitors TRUSTOPIA Services for unauthorised intrusions using network-based intrusion detection mechanisms.

TRUSTOPIA may analyse data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications and to ensure that TRUSTOPIA Services function properly.

Security Logs

TRUSTOPIA systems used in the provision of TRUSTOPIA Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralised syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

TRUSTOPIA maintains security incident management policies and procedures. TRUSTOPIA promptly notifies impacted customers of any actual or reasonably suspected unauthorised disclosure of their respective Customer Data by TRUSTOPIA or its agents of which TRUSTOPIA becomes aware to the extent permitted by law.

TRUSTOPIA maintains Cyber and Data Risk Insurance with Hiscox.
User Authentication

Access to TRUSTOPIA Services requires authentication via one of the supported mechanisms including user ID/password, SAML based Federation, and Oauth. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

The TRUSTOPIA Services include a variety of configurable security controls that allow customers to tailor the security of the TRUSTOPIA Services for their own use. All communications with the platform are encrypted over SSL and authentication is handled using the industry standard protocol, OAuth 2.

OAuth 2 is an authorisation framework that enables applications to obtain limited access to user accounts on an HTTP services and is utilised by companies such as Twitter and Facebook. It works by delegating user authentication to the service that hosts the user account, and authorising third-party applications to access the user account. OAuth 2 provides authorisation flows for web and mobile applications and this is why it is the perfect solution for TRUSTOPIA.

Physical Security

The Amazon Web Service production data centres used to provide TRUSTOPIA Services have access control systems. These systems permit only authorised personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilise redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems and are secured by around-the-clock guards, two-factor access screening, including biometrics, and escort-controlled access. They are also supported by on-site back-up generators in the event of a power failure.

Planned System Updates

Updates are made available to all users of the platform and are automatically applied at development milestones which are communicated in advance. Given that the platform is continually evolving TRUSTOPIA normally expects to have 3-4 major updates each year with more frequent bug fix releases made as and when required.

The update process is a seamless process and most users with automatic updates switched on will not even notice the process. For users who prefer to apply updates manually they will be prompted to update their application.

For sizeable updates to the TRUSTOPIA Portal it can be that some outage might occur so therefore updates are scheduled in advance and where possible updates are applied outside of working hours, during the evenings and or at weekends.

Standard System Support Services

The TRUSTOPIA systems support team is available during business hours Monday – Friday: 0930 – 1700.
TRUSTOPIA provides its customers with designated contact number(s) and email address(es) for system support contact points which are the contact points for reporting faults and making enquiries relating to the services.

Response is determined in the table here:

<table>
<thead>
<tr>
<th>Escalation</th>
<th>Availability</th>
<th>Target SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Ticket</td>
<td>During business hours</td>
<td>90% of escalations (or attempts to escalate) completed within 2 business days</td>
</tr>
<tr>
<td>Telephone Support</td>
<td>24 hr / 365 days per year</td>
<td>90% of tickets completed within 4 business hours</td>
</tr>
<tr>
<td>Email Support</td>
<td>24 hr / 365 days per year</td>
<td>Manned telephone support available during business hours. Answer phone available outside of business hours with redirection to on-call team members.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>95 % of all emails responded to within 2 business days.</td>
</tr>
</tbody>
</table>

SLA’s are monitored and statistics shared with customers at account management meetings.

System Availability

The production system is available 24 hours a day, 365 days a year, subject to planned maintenance or in the event of major system failure.

The TRUSTOPIA system has been designed to provide a high level of resiliency to reduce the potential impact of major outages.

TRUSTOPIA’s Operational Target level for system availability is an average of 99.4 % over any rolling 3 month period (including planned maintenance) excluding any unplanned outage.

Planned or Scheduled Maintenance

From time to time, TRUSTOPIA will need to schedule maintenance of its services. TRUSTOPIA will always endeavour to conduct planned maintenance at a time that reduces the impact on the availability of the service. So, where possible, planned maintenance will be conducted during low usage periods outside of business hours. If the Service needs to be suspended for planned maintenance, as much advance notice as is practicable is provided.

Change Management

TRUSTOPIA manages an on-going change management programme to further enhance its applications, services and systems. These changes may be as result of internally identified changes, legislative changes driven by external bodies, or by customer requests.

Change requests are considered as part of an internal change management process. Where applicable change requests will be consolidated into packages for the release through the planned or schedule maintenance outlined above.
Please note all planned changes will upgrade all client systems simultaneously to ensure all platforms comply with the latest guidelines / legislation. Change management is provided as standard as part of the subscription service fees.

Service Management

Day to Day System administration: Regular and periodic system administration tasks are included within the service and are a mixture of automatic and manual tasks. These administration tasks are reviewed and updated on a regular basis. These include, but are not limited to, application, network and security monitoring.

Issue Resolution: TRUSTOPIA responds to faults we detect or which clients report via the support service. These faults are logged and categorised according to severity detailed in the table below.

TRUSTOPIA offers target response times as described below as part of the standard support service:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Impact</th>
<th>Target Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 1</td>
<td>The Service is not operational or is inaccessible</td>
<td>80% of faults cleared within 1 day from acknowledgement of the fault.</td>
</tr>
<tr>
<td>Severity 2</td>
<td>Service is degraded, a marked increase in time to access the Service. A problem causing significant reduction in functionality</td>
<td>80% of faults cleared within 3 days from acknowledgement of the fault.</td>
</tr>
<tr>
<td>Severity 3</td>
<td>The Service is experiencing minor problems but is functioning substantially</td>
<td>80% of faults cleared within 5 Business Days from acknowledgement of the fault.</td>
</tr>
<tr>
<td>Severity 4</td>
<td>Minor problem with the Service but does not impact the Client’s use of the Service</td>
<td>Fixes made available in future release of the software.</td>
</tr>
</tbody>
</table>

Reliability and Backup

All networking components, SSL accelerators, load balancers, web servers and application servers are configured in a redundant configuration.

All Customer Data submitted to the TRUSTOPIA Service is stored on a primary public cloud infrastructure database server with multiple active clusters for higher availability.

All Customer Data submitted to the TRUSTOPIA Service, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and is backed up on a regular basis and stored on backup media for an additional 35 days in
production environments and 30 days in Sandbox environments after which it is securely overwritten or deleted from the TRUSTOPIA Service.

TRUSTOPIA uses Amazon Relational Database Service (Amazon RDS) to provide a relational database in the cloud, providing capabilities of a familiar MySQL, MariaDB, Oracle, SQL Server, or PostgreSQL database. Amazon RDS automatically patches the database software and backs up the database, storing the backups for a user-defined retention period.

Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. Reverting to an earlier DB snapshot in the event of a data issue can be tackled very quickly and with minimal downtime.

Disaster Recovery

TRUSTOPIA has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data center to the secondary data center utilising developed operational and disaster recovery procedures and documentation.

TRUSTOPIA Process-As-A-Service disaster recovery plan has the following target recovery objectives:

(a) restoration of the TRUSTOPIA Service within 12 hours after TRUSTOPIA’s declaration of a disaster; and
(b) maximum Customer Data loss of 4 hours; excluding, however, a disaster or multiple disasters causing the compromise of both data centers at the same time, and excluding development and test bed environments, such as the Sandbox service.

TRUSTOPIA’s chosen public cloud infrastructure partner – Amazon Web Services – has been chosen by TRUSTOPIA to mitigate the risk of single points of failure and provide a resilient environment to support TRUSTOPIA service continuity and performance.

TRUSTOPIA makes use of Amazon’s Multi-AZ support for Amazon RDS for SQL Server which provides for an immediate fail back to a mirror of the current database in the event of a database failure. This high availability option leverages SQL Server Mirroring technology with additional improvements to meet the requirements of enterprise-grade production workloads running on SQL Server.

The Multi-AZ deployment option provides enhanced availability and data durability by automatically replicating database updates between two AWS Availability Zones. Availability Zones are physically separate locations with independent infrastructure engineered to be insulated from failures in other Availability Zones.

Amazon RDS automatically provisions a primary database in one Availability Zone and maintain a synchronous "standby" replica in a different Availability Zone. In the event of planned database maintenance or unplanned service disruption, Amazon RDS will automatically fail over the SQL Server database to the up-to-date standby so that database operations can resume quickly, without any manual intervention.
Viruses

TRUSTOPIA Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the TRUSTOPIA Services by a customer. Uploaded attachments, however, are not executed in the TRUSTOPIA Services and therefore will not damage or compromise TRUSTOPIA Services by virtue of containing a virus.

Data Encryption

TRUSTOPIA Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the TRUSTOPIA Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Additionally, all data, including Customer Data, is transmitted between data centers for replication purposes across a dedicated, encrypted link utilizing AES-256 encryption.

Return of Customer Data.

Within 30 days of contract termination; customers may request return of their respective Customer Data as submitted to a TRUSTOPIA Service (to the extent such data has not been deleted by Customer). TRUSTOPIA shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format.

Deletion of Customer Data

After contract termination, Customer Data submitted to the TRUSTOPIA Services is retained in inactive status within the TRUSTOPIA Services for 120 days after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days.

Physical media on which Customer Data is stored during the contract term is not removed from the data centers that TRUSTOPIA uses to host Customer Data unless the media is at the end of its useful life or being deprovisioned, in which case the media is first sanitised before removal. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the TRUSTOPIA Services, TRUSTOPIA reserves the right to reduce the number of days it retains such data after contract termination. TRUSTOPIA will update this TRUSTOPIA Security, Privacy, and Architecture Documentation in the event of such a change.

Tracking and Analytics

TRUSTOPIA may track and analyse use of the TRUSTOPIA Services for purposes of security and helping TRUSTOPIA improve both the TRUSTOPIA Services and the user experience in using the TRUSTOPIA Services.
TRUSTOPIA may also use this information and users’ e-mail addresses to contact customers or their users to provide transactional information about the TRUSTOPIA Services. TRUSTOPIA will offer customers and users the ability to opt out of receiving such emails.

Without limiting the foregoing, TRUSTOPIA may share anonymous data about TRUSTOPIA’s customers' or their users' use of the TRUSTOPIA Services (“Usage Statistics”) to TRUSTOPIA’s service providers for the purpose of helping TRUSTOPIA in such tracking or analysis, including improving its users’ experience with the TRUSTOPIA Services, or as required by law.

Additionally, TRUSTOPIA may share such anonymous data with other customers on an aggregate basis. Except when required by law, any such sharing of Usage Statistics will not include any identifying information about TRUSTOPIA’s customers or customers' users.

Interoperation with Other TRUSTOPIA Services.

TRUSTOPIA Services may interoperate with other services provided by TRUSTOPIA or third parties.

Further Information

If you wish to understand more: AWS provides certification reports that describe how the AWS Cloud infrastructure meets the requirements of an extensive list of global security standards, including: ISO 27001, SOC, the PCI Data Security Standard, FedRAMP, the Australian Signals Directorate (ASD) Information Security Manual, and the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584).

For more information about the security regulations and standards with which AWS complies, see the AWS Compliance webpage.