TRUE COMPLIANCE

Data Security Policy

Authored by: Graeme Kilkenny
On: 18th June 2021
To be reviewed by: 18th Dec 2022

Aim

The aim of True Compliances data security policy is to twofold. Firstly, to prevent unauthorised access or distribution of data entered into the application. Secondly, to maintain the persistence, integrity and availability of the data to legitimate users.

Overview

True Compliance is hosted on the Amazon Web Services (AWS) platform. The data is stored in the London data centre. We use the RDS service to provide the database servers, and the S3 service as a file store. We also have an offline set of backup disks. Amazon are well known for the high level of physical security they employ at their data centres. It is highly unlikely that any physical theft would happen onsite.

Data for our purposes is comprised of the database, and the copies of all the certificates that have been loaded into True Compliance.

Access

Users can access the certificates, and database data via the frontend application at truecomp.co.uk. Access to this system is secured via password protected accounts. The authentication system is managed by third party experts Auth0. Accounts are granted centrally by True Compliance at the request of our clients, and clients can then add and remove users as they see fit. True Compliance also integrates with their own user management systems (Active Directory, Google Suite etc) to allow them easier control of their user base. You cannot sign up online for access. User accounts are removed once no longer active. The True Compliance website is securely hosted over a https connection. All

reasonable attempts are made to protect the sites codebase from malicious external attacks.

True Compliance runs on a serverless platform, and as such there are no physical servers to protect. Access to the Lambda functions or server less databases is achieved either via AWS, or via our hosting management portal.

Access to the AWS console is limited to the responsible staff within True Compliance, and privileges are assigned to users on an individual basis. Full access is restricted to the CTO. Access to other services is granted to users based on operational need, and reviewed regularly.

Integrity

To handle against the unlikely possibility of catastrophic failures, True Compliance maintains multiple cross location backups.

Database: The database is backed up with the AWS infrastructure. An exact point in time backup is available for any time within the last seven days. We also retain weekly offline backups to mitigate against catastrophic loss.

Certificates: The certificates are stored on S3, which is automatically backed up by Amazon to prevent loss from hardware failure.

Codebase: The application codebase is stored in repositories kept in the Gitlab cloud repository store, as well as on our servers and local development environments.

As a result True Compliance has no single point of failure when it comes to data integrity.

Disaster Scenarios

1) Amazon: The worst case scenario. If Amazon were to go out of business, or the data centre suffers a catastrophic incident, then we can relocate our server base to another AWS location / another

server provider entirely. Our codebase is stored with a separate service, and our data can be recovered from the physical backup.

Likelihood of occurrence: Extremely unlikely
Potential Data Loss: Up to 24 hours
Downtime: Up to 24 hours

2) True Compliance Office: If our office were to be flooded or burn down, or we otherwise suffered mass loss of hardware / equipment. In this scenario, we just need to re-equip the office. The codebase / live servers / data stores are all offsite. We may lose some physical backups, but these could be replaced from the live data.

Likelihood of occurrence: Unlikely
Potential Data Loss: None
Downtime: None

3) Gitlab: If we somehow lost the use of Gitlab as a service provider. This would be the lowest level of risk. We'd just switch to another service, using one of the copies of the codebase available across the live and staging platforms, and also locally available.

Likelihood of occurrence: Unlikely
Potential Data Loss: None
Downtime: None

4) Server or Database failure: TC runs a server less infrastructure. Were one of our function calls to fail others would be invoked to handle the traffic load. There is no persistent hardware that can fall over. If something doesn’t work it will be immediately replaced.

Likelihood of occurrence: Probable
Potential Data Loss: None
Downtime: None

GDPR Appendix

Personal data stored on True Compliance is limited solely to the names (and sometimes telephone numbers) of residents, and the address to which that name is associated.

This data is acquired from our clients who have the legal right to compile and hold information about their residents and use third party systems to administer that data.

True Compliance does not, and will never share any information held on our servers with any party except the client that put it there, as part of their normal business practices.

We store compliance data for three years. After this period, all information (including residents names) will be deleted.

If a resident makes a specific request to us at support@truecompliance.co.uk, will we remove their name / number from the system within 10 working days, except in cases where doing so would be in breach of our clients legal right to retain this information, and they have specifically asked us not to. Either way the resident shall be informed.

True Compliance does not share, process, profile or track any of the residents whose names are stored, nor do we have any mechanism by which we could do this. The residents names are not matched to any other dataset, and exist only as a data point against the specific compliance record / property loaded into the system.

As the personal data is limited to named social housing tenants, there is no data relating to children in the system.

We do not collect data relating to financial payments, medical issues, sexual orientation, religious affiliation, or indeed any personal information apart from that noted above.