SCRIBE

Data Security and Compliance

Publicly Available Overview

Sensitive information has been removed from this document so that it may be shared with Scribe customers

Authors

Wayne Taylor, CTO

John Swindells, Senior Engineer

John Fagan, CEO

Contents

Overview **4**

Personal data 4

Communications and operations management **5**

ISO 27001 5

PCI 5

Service management 5

Change management 5

Incident management 5

Security Audit 5

Disaster Recovery **6**

Emergency Contacts 6

Comms Plan 6

HIGH severity issue communications 6

CRITICAL severity issue communications 6

Communication strategy 7

Systems Recovery 8

Customer Support 8

CRM System 8

Password Access 8

Technical Recovery (app.scribeaccounts.com) 9

Webservers - Elastic Beanstalk (EB) 9

Resetting EB 9

Relational Database Service (RDS) 9

Resetting RDS 9

Recreating RDS 9

Dynamo DB 9

Recreating Dynamo DB 10

Infrastructure **11**

Availability 11

Overview 11

Hosting 11
Geography 11
Cloud service connections 11
Technical security measures **12**
Network 12
Anti-virus 12
Transport 12
Penetration testing 12
Password policy 12
Access 12
Secure coding practices 13
Data storage and retention **14**
Shared tenancy 14
Backup 14
Data Retention 14
Removal of data 14
Asset management 14
Physical and environmental security **15**
Access 15
Mitigating the impact of loss, damage or stolen equipment 15
Human Resource Security **16**
Data protection policy 16
Pre-employment checks 16
Employment contracts 16
Employee offboarding 16
Customer obligations **16**
Privacy policies 16
Other **16**
Copyright, designs and patents act 1988 17

Overview

Scribe is a web-based information management system for UK-based councils. As such, it stores council data online. A council's data is generated by authorised council personnel, Scribe's Professional Services team and the council's own customers.

In a number of places sensitive information and overly technical details have been removed from this version of this document to tailor it for Scribe customers.

Personal data

We collect & store the personal information of Scribe customers (eg, council employees and councillors) and also the personal information of their suppliers & customers. These are critical requirements for the delivery of Scribe's services.

Access to all personal information is defined by Roles within Scribe. Each Role relates to specific parts of council operations and may be read-only or read-write.

You may withdraw your consent to us processing your personal data at any time by notice in writing to us. Following the withdrawal of your consent, we will cease further processing of your personal data other than in respect of the information that we are required to retain including, but not limited to payment information and gift aid data which will be required for the periods legally required.

https://www.scribeaccounts.com/privacy

Communications and operations management

ISO 27001

All of our technical infrastructure is hosted by Amazon in compliance with ISO 27001. https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf.

We have many processes and policies in place which are in line with ISO 27001. We take the protection of information very seriously and aim to obtain formal accreditation for our operational processes in the future.

PCI

Scribe processes payments using PCI compliant 3rd Party processors such as Stripe. No Card details pass through our systems and as such PCI is not applicable.

Service management

We do not use ITIL but we make use of an Agile Continuous Improvement process. This is based on user demand and focuses on delivering improvements by incremental change. Regression testing is used to minimise any risk during upgrades.

Change management

We make use of an Agile software development process. As part of this process, we analyse business and operational risk during planning and implementation. Development and staging environments are in place to test any changes prior to being made on the live site. Software updates are usually made without any downtime. If significant downtime is required to update the software then this is communicated to the account holder ahead of the update being deployed.

Incident management

Data breaches are investigated for the root cause. Controls are deployed to mitigate the further impact. Any incidents will be reported to the Scribe account owner via email. Our target for communicating this is 36 hours.

Any breaches to data which Starboard Systems Ltd is the data processor will be reported to the UK Information Commissioner's Office (ICO) by the Data Protection Officer.

Security Audit

Scribe account owners and any users with the 'User Management' permission can view details of which users have access to their account.

Disaster Recovery

Emergency Contacts

A WhatsApp group has been set up for disaster recovery communications and to alert the team. Below is a list of key contacts as a fallback.

NAME	ROLE	EMAIL	TEL
[REDACTED]			

Comms Plan

Regular contact should be made with the main POC for each council. Coms should be treated in 2 tiers based on the severity of the issue:

- HIGH - partial outage
- CRITICAL - complete outage and or potential data loss

Templates and drafts are available for each communication channel to ensure quick, efficient and accurate communication. The full version of the document details steps on how to activate each of these.

HIGH severity issue communications

- Setup VoiceMail on the phone system
- Email
- Email Auto Responders
- Facebook (Scribe Family)
- Twitter
- Website banner and link to blog

CRITICAL severity issue communications

- Setup VoiceMail on the phone system
- Email
- Email Auto Responders
- Facebook (Scribe Family)
- Twitter
- Website banner and link to blog

Communication strategy

A communications strategy is in place to ensure clear communication with customers

Systems Recovery

Our business is built around flexible working and all our infrastructure is securely hosted online. Interruption to activity is mitigated as support systems (ticket management, CRM) are cloud-based and can be accessed from mobile devices.

Customer Support

We use a highly available, cloud based Customer Support platform. In the unlikely event of an extended outage, customer contact information and history can be retrieved and responded to from GMail, the underlying email client.

CRM System

We use a highly available, cloud based CRM. In the unlikely event of an extended outage, customer contact information and history can be retrieved from GMail, the underlying email client.

Password Access

A password manager is used to securely store passwords across the business. In case of an outage, passwords are cached on mobile devices and laptops. To mitigate this all staff are to install the 1Password app on desktop and mobile.

Technical Recovery (app.scribeaccounts.com)

Scribe Apps are hosted using Amazon Web Services using good practices for availability, resilience and backups.

Webservers - Elastic Beanstalk (EB)

EB is a managed service that is used to run the webservers that host Scribe Apps. EB auto scales to match spikes in demand and will automatically replace web servers if they become unavailable.

Resetting EB

In the event of an issue with EB the first step should be to rebuild the existing EB environment:

Recreating EB

In a highly unlikely worst case scenario of an extended period of downtime across the whole of the AWS London data centre, the following process can be used to start a new replica Scribe environment:

Relational Database Service (RDS)

RDS is a managed database service that we have configured to have a point-in-time recovery with an accuracy of 5 minutes as well as monthly backups.

Resetting RDS

In the event of an unresolvable issue with RDS the first step should be to restart the database. Please note that during the restart process web servers are not able to connect to the database and this can cause a build up of requests on the web servers that can lead to EB needing to be restarted.

Recreating RDS

In a highly unlikely worst case scenario of an extended period of downtime across the whole of the AWS London data centre or if the database needs to be completely restored then the following process can be used to start a new replica Scribe database based on a point-in-time.

Dynamo DB

Dynamo is a fast, flexible NoSQL database service for single-digit millisecond performance at any scale For tables using provisioned capacity, DynamoDB delivers automatic scaling of throughput and storage based on your previously set capacity by monitoring the performance usage of your application. If your application traffic grows, DynamoDB increases throughput to accommodate the load. If your application traffic shrinks, DynamoDB scales down so that you pay less for unused capacity.

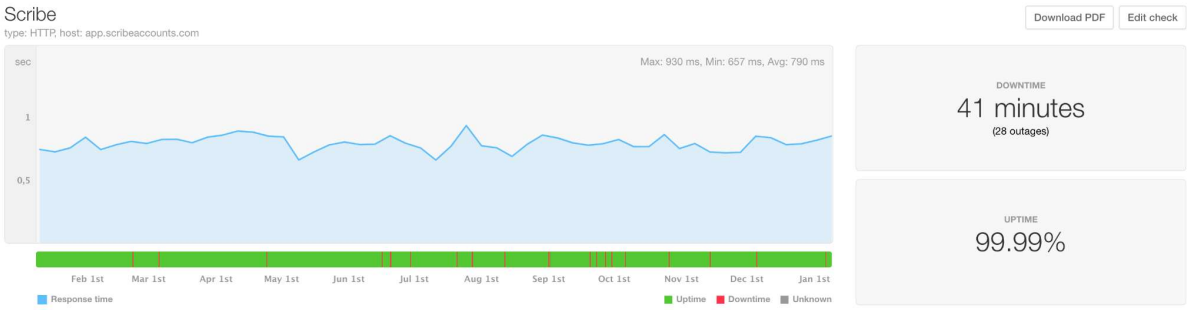
Dynamo DB is used for storage of non-essential logging information.

Recreating Dynamo DB

Infrastructure

Availability

Scribe is a High Availability System. Daily backups are made and 5-minute point in time recovery is available for platform data. Although we do not have SLAs related to availability, during 2022 we had a 99.99% uptime.



Overview

Scribe consists of web servers and database storage within an AWS virtual private cloud (VPC). An AWS load balancer is the public-facing endpoint for accessing the Scribe web service. This endpoint is accessed by the public via a Cloudflare proxy/firewall service. AWS Identity & Access Management (IAM) is used to control access to individual resources.

Hosting

Data is hosted in Amazon Web Services (AWS). Amazon provides leading information security capabilities see https://aws.amazon.com/security/. Customer data security terms are NOT passed on to AWS.

Geography

All Scribe data is hosted in London.

Cloud service connections

Cloud service connections are recorded and maintained in AWS.

Cloud service connections are tested upon initiation.

Staff usage of cloud services is recorded and maintained in AWS using IAM roles.

All connections are served over SSL (using TLS v1.3).

Technical security measures

Network

Scribe data are hosted in a Virtual Private Cloud (VPC). Our database is only accessible from within this VPC. Ports are restricted, so web servers can only be accessed by HTTP(s). RDP access is only available from several restricted IP addresses.

Network configuration is controlled via Amazon Web Servers. Webserver configuration is controlled using Elastic Beanstalk.

Anti-virus

Microsoft Security Essentials is included on our servers and is updated periodically and upon any urgent requirements.

Encryption

Platform data is encrypted in transit when accessed via Scribe GUI interface over a Secure Sockets Layer (SSL) connection, using HTTPS TLS v1.3.

User credentials (passwords) are encrypted at rest using HMAC-SHA256.

Penetration testing

We conduct periodic in-house penetration testing.

In order to ensure a comprehensive test has been performed the coverage of tests is recreated each year prior to running the test. Testing is currently performed using the latest version of OWASP ZAP, though this is reviewed each year.

Each system is tested by manual site exploration followed by a Spider and Full Active Scan. Systems are tested using crawler techniques with exploration aided by manual use of the system to help with URL discovery. The system can change a lot over 12 months, so it is important that testing is performed from scratch rather than rerunning the previous tests or repeating a fixed script.

Scanned URLs, parameters, and responses for each system are recorded to CSV. These tests are retained so they can be compared to the previous year's tests to ensure test coverage has not degraded.

High-Risk issues are acted upon as top priority and are deployed immediately.

Medium Risk issues are added to the current sprint cycle and deployed as part of the next planned software update.

We can provide a replica environment for clients to perform security testing on. Fees apply to cover provisioning and hosting costs.

Password policy

Complex passwords are encouraged, and use of company M=Password Manager is required for password management.

Access

Access to Scribe administration, CRM and internal systems are managed using roles and permissions. This ensures that users only have access to the information they are authorised to view.

Internal systems are securely cloud-hosted and access is managed using roles and permissions. This ensures that users cannot make unauthorised changes to computers or applications. Staff usage of cloud services is recorded and maintained in AWS using IAM roles. All connections to cloud services are served over SSL.

Secure coding practices

Software designed with security in mind. OWASP Secure Coding Practices are reviewed as part of penetration testing outcomes and human feedback (in-house or third-party).

Data storage and retention

Data Protection Officer – **John Fagan.**

Shared tenancy

Customer project data is stored on a shared database in the cloud. Data is stored against a unique ID per account and protected with password access. Grey box testing is performed as part of release testing to ensure no data is visible from other accounts.

Backup

Daily backups are retained for 30 days. Monthly backups are retained for 6 months. 5-minute point in time recovery is available for platform data.

Data Retention

The customer is in full control of the customer data stored through the Scribe SaaS service and has the responsibility to determine the retention scheme for the customer data.

Removal of data

The Scribe contract specifies that customer data will be available in an industry-standard format for download upon termination or completion of the service (free of charge). Except as otherwise agreed or required by applicable law, the customer will have 30 days to download such data before it is deleted and, thereafter, all such customer data (including backups) will be cycled out of the SaaS service systems and deleted within 180 days.

Asset management

Scribe maintains a register of all IT and Information assets (see appendix)

Physical and environmental security

Access

Our office is physically protected by electronic key fob access during working hours and also physical key overnight. 24/7 CCTV in place.

Mitigating the impact of loss, damage or stolen equipment

Our business is built around flexible working and all our infrastructure is securely hosted online. Interruption to activity is mitigated as support systems (ticket management, CRM) are cloud-based and can be accessed from mobile devices.

Human Resource Security

Data protection policy

We take data security very seriously and therefore review the policy ahead of running staff training sessions. Staff training sessions are delivered periodically. Training records are recorded within Google Forms.

Pre-employment checks

Proof of address information and identification documents are validated for all staff and references provided.

Employment contracts

Data protection, security and confidentiality clauses are included in employment contracts.

Employee offboarding

Exit interview and leavers checklist are completed as part of the offboarding process. Leavers checklists are signed off by a key member of each relevant department to ensure that when people leave the organization their access to systems is disabled or removed.

Customer obligations

Scribe can be utilised to help our customers comply with their data protection obligations. It is important to distinguish that Starboard Systems Ltd acts as a Data Processor and holds information that our customers have collected utilising our services. Where we hold data on our customer's behalf, they are usually the data controller and therefore are responsible for making decisions about lawful processing and complying with individuals' rights. Scribe provides features to help customers stay compliant and are responsible for ensuring the security of the data that we store.

Privacy policies

A privacy policy and terms and conditions link can be displayed on the consumer-facing Bookings page. Simply enter the URL of your privacy policy and terms in the Bookings settings page and a link will automatically be shown on all of your councils' consumer-facing bookings pages.

Other

Copyright, designs and patents act 1988

Starboard Systems indemnify the Customer from and against all losses which are suffered by the Customer if its use of the Service infringes the Intellectual Property Rights of any third party (Supplier IPR Claim). Full details and exceptions are available in our terms and conditions.