Evo Security Statement & Backup Policy

Backups
It's crucial we keep backups of our core production data, so in the event of major failure (like a coding error that erases customer data from the database) we can roll back to a previous safe state.

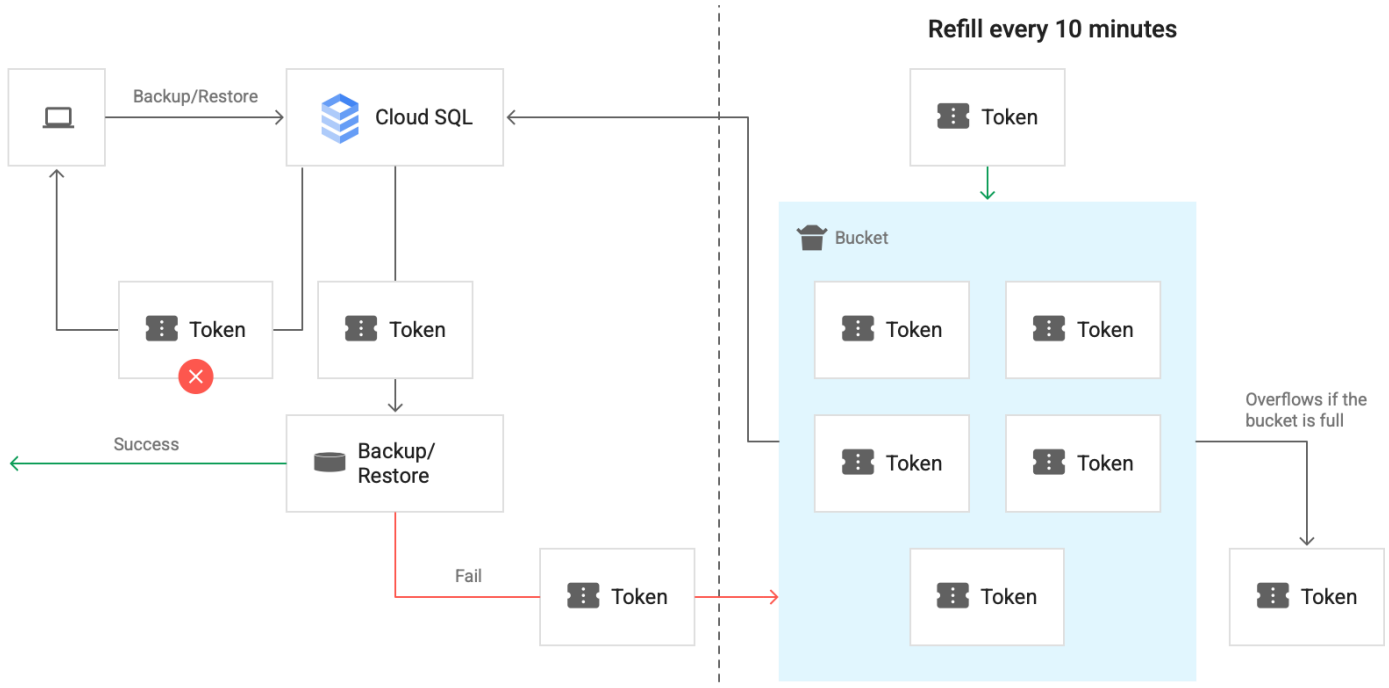
Requirements
- We take daily snapshots of all production data and store it on an independent system.
- Receive automated notifications if/when a backup is unsuccessful.
- We replay backups frequently to ensure they are still working and check data integrity.
- Ensure backups are archived on a schedule.

Implementation
- The Evo application runs in Google Cloud App Engine, the live database being in Google Data Store. Our backups are stored in the Google Cloud Storage service, which is entirely independent from the Live Production environment. Even if a coding error or App Engine related problem, led to our entire database being wiped, we'd be able to recreate the database within hours.
- A daily notification email is sent to key employees when a backup has been taken, and in case anything in the process has failed the email states this very clearly in the subject line, and we'll take immediate action to ensure the backup will work.
- At least every 2 months we take a backup and replay it onto an empty server and ensure the process still works.

Replication

Goal
- It's important that we don't have a single point of failure. All our production systems need to survive individual servers or even entire data centers going down.

Implementation
- We run all our crucial production systems in the Google Cloud. Most services have cross-datacenter replication built in by default (our database and production servers for instance). In the few cases where we have to build our own infrastructure like our Google-hosted Load balancers, or our Google-hosted PDF-generation-servers, we ensure that there is always enough replication in place for single servers or even datacenters to fail without jeopardising the service itself.



At Evo we make it a priority to take our users' security, privacy, and data integrity concerns seriously. We strive to ensure that user data is kept securely, backed up safely and that we collect only as much personal data as is required to provide our services to users in an efficient and effective manner.

Evo uses some of the most advanced technology for Internet security that is commercially available today. This Security Statement and backup policy is aimed at being transparent about our security and integrity infrastructure and practices, to help reassure you that your data is appropriately protected.

Data Backup and Retention

General

- Daily Backup: Incremental backups are performed daily within each user's account of all the data in that account. This backup forms part of the data-usage of the account. This type of backup can be switched off in the subscription settings. A daily incremental backup is also taken of the entire Evo system, which is kept on both the Evo server and are copied to a geographically separate, secure server
- Periodic Backups: Full Weekly and Monthly backups are taken of the entire Evo system, and these are kept on a separate secure server
- Independent backup: We advise that you take regular backups independently and download any data that might be critical to your organization. This is purely as a last line of defence.

Accessible Data/Archive

- Your Data: For an active account that is within its limits of users, instruments and data-storage, your data will continue to be made available to you without archiving or removal.

File Restoration Methods and Timeframe

- User Account Backup: The backup made automatically within your account will be available to you to restore and can be accessed through your account. You will not be able to restore any data lost since the last backup.
- System Backup: If you need to recover data and do not have a user account backup, you will need to contact Evo to request your data to be restored. You can contact us at support@evo.pm

Backup Technologies

- User accounts with data are backed up within the Evo software system using internal file creation scripts.
- Full system backups are created on the Evo cloud server using a server-based database backup system.
- Last-line-of-defense-backups are created using Server to Server (STS) backup via an Authenticated Backup Protocol (ABP). These are located on an independent, secure Server.

Application and User Security

- SSL/TLS Encryption: All user interactions with Evo are done over a Secure Socket Layer (SSL) connection which protects communications by using both server authentication and data encryption. This ensures that user data in transit is safe, secure, and available only to intended recipients.
- User Authentication: User data on our database is logically segregated by account-based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on. Evo issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the password of the user.
- User Passwords: User application passwords have minimum complexity requirements. Passwords are individually salted and hashed.
- Data Encryption: Certain sensitive user data, such as account passwords, is stored in encrypted format. Credit card information is held independently by https://revolut.com our payment provider.
- Data Portability: Evo enables you to export your data from our system in a variety of formats so that you can back it up or use it with other applications.
- Privacy: We have a comprehensive privacy policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

Physical Security

Data Centers: Our primary servers run on Google Cloud - Cloud SQL automatically ensures our databases are reliable, secure, and scalable so that our business continues to run without disruption. Cloud SQL automates all our backups, replication, encryption patches, and capacity increases—while ensuring greater than 99.95% availability, anywhere in the world.

- Located in a Tier 3, ISO certified data center in London, United Kingdom and is designed using the latest technology to specifically guarantee powerful performance, reliability, and security.
- Data encryption at rest and in transit. Private connectivity with Virtual Private Cloud and user-controlled network access with firewall protection. Compliant with SSAE 16, ISO 27001, PCI DSS, and HIPAA.
- Redundancy: Multiple levels of redundancy have been built in to ensure consistent high performance, including multiple paths for cooling and power distribution with emergency backup generators ready to start in the event of power loss.

Software Development Practices

Coding Practices: Our engineers use best practices and industry-standard coding guidelines to ensure secure coding using our 5 core principles of Dependability, Efficiency, Maintainability, Simplicity and Usability.

Network Security

- Security Policies: The server is also fully compliant with the latest security policies and audit guidelines, with a meticulous approach to ensuring private data stays private and protected at all times.
- Security Monitoring: All files stored on the server are continuously monitored for potential security breaches with immediate warning to us in the event of a suspicious file being added or altered.

Organisational & Administrative Security

- Training: We provide security and technology use training for relevant employees.
- Service Providers: We screen our service providers and bind them under contract to appropriate confidentiality obligations if they deal with any user data.
- Access: Access controls to sensitive data in our databases, systems and environments are set on a need-to-know / least privilege necessary basis.

Payment Systems

- Online Payments: We use https://revolut.com for payment processing on Evo for the purchase and renewal of subscriptions.
- Direct Debit: We use https://gocardless.com for processing and managing Direct Debit Payments for plans and one-off payments.

Handling of Security Breaches

Despite best efforts, no method of transmission over the Internet and no methods of electronic storage are perfectly secure. We cannot guarantee absolute security. However, if Evo learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under UK law, as well as any industry rules or standards that we adhere to. Notification procedures include providing email notices or posting a notice on our website if a breach occurs.

Our Responsibilities

Evo users have a responsibility to ensure Evo and Customers data is securely maintained and available for backup.

Users must not store data/files on the local drive of a computer (this excludes the normal functioning of the Windows or MacOS operating system and other authorized software which require the 'caching' of files locally in order to function). Instead, Users must save data (files) on their allocated areas – this could be within the EDRM system, a mapped drive or network shared folder the user has access to. Data (files) which are stored "locally" will NOT be backed up and will therefore be at risk of exposure, damage, data corruption or total loss.

Your Responsibilities

Keeping your data secure also depends on you ensuring that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems, to keep any data you download to your own computer away from prying eyes. We offer SSL/TLS certification to secure the transmission of data, but it is your responsibility to ensure that your systems are configured to use that feature where appropriate.

Technical Support

Evo Digital Technologies Limited (Evo) aims to provide a primary approach in supporting our customers and users via the FAQ's section on our website at https://www.evo.pm/help To ensure we are constantly achieving best-in-class CSAT, users can contact us directly via our interactive Chat Widget on our website. We have implemented response times based on the severity of the issue reported, as defined by the Priority Levels detailed within our SLA documentation.

Evo runs on Google Cloud Platform which guarantees 99.5% uptime availability.

Hours of Operation (GMT/BST)

Standard Support Monday – Friday 9am – 5pm

- ShowStopper
  - Anticipated response within 2 hours from time of receipt.
- Priority1
  - Anticipated response within 24 hours from time of receipt.
- Priority2
  - Anticipated response within 3 days from time of receipt.
- Priority3
  - Anticipated response within 5 days from time of receipt.
- Priority4+
  - Anticipated response within 7 days from time of receipt.

Optional Non-Standard Support Hours*

Weekday evenings 5pm – 8pm, Weekends 10am – 4pm

- ShowStopper Only
  - Anticipated response within 6 hours from time of receipt.

**Optional Non-Standard Support Hours are offered as a premium, chargeable service.*

Lines of communication

1. WebChat (if not accessible for any reason, then contact us via the following methods in order.
   a. Email to support@evo.pm
   b. SMS +44 (0)7400 079293
   c. WhatsApp +44 (0)7723 502080
   d. Call +44 (0) 20 8691 9293, option 9