SECURITY OVERVIEW

In Case of Crisis
by RockDove Solutions

At RockDove Solutions, the protection and privacy of your company and end-user data is one of our top priorities. We have built an enterprise mobile solution that offers end-to-end encryption and much more. In this brief document, we outline some of the highlights of our commitment to your security.

Our sites are protected with TLS 1.2 using SHA-2, as a minimum encryption standard. Additionally, our sites are hosted using Cloud Providers who pride themselves in providing confidentiality, reliability, and availability.

When you sign in to the In Case of Crisis customer portal, your plan and account information are protected with passwords that are salted and encrypted with a one-way hash algorithm (SHA-2), and the hashed value is used to construct a new hash value which is then compared to the value stored within the secure database. In this way, no one can view the user passwords and in the event of a security breach, the passwords would be of no value and would be un-intelligible.

Database access is restricted via IP filtering to our team of database administrators. All communications between the database and web server are encrypted and the complete data store is encrypted at rest through Microsoft Azure Transparent Data Encryption (TDE), using AES-256.

All admin access to the In Case of Crisis hosting servers requires Multi-factor authentication using Google Authenticator, is IP filtered and audit logs are maintained and reviewed to ensure authorized access only to restricted services. The protocol for remote access is Microsoft Windows Remote Desktop Protocol (RDP) using Google Authenticator services.

CLOUD-BASED HOSTING SERVICES

In Case of Crisis web services is provided by Amazon EC2 within their Eastern Region. Amazon was the third cloud services provider to be certified by the Federal Risk and Authorization Management Program (FedRAMP). This certification means that Amazon can help Federal agencies scale new cloud solutions quickly and securely.

➡ **Additional Information:** AWS has in the past successfully completed multiple SAS70 Type II audits, and now publishes a Service Organization Controls 1 (SOC 1), Type 2 report, published under both the SSAE 16 and the ISAE 3402 professional standards as well as a Service Organization Controls 2 (SOC 2) report. In addition, AWS has achieved ISO 27001 certification, and has been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). In the realm of public sector certifications, AWS has received authorization from the U.S. General Services Administration to operate at the FISMA Moderate level, and is also the platform for applications with Authorities to Operate (ATOs) under the Defense Information Assurance Certification and Accreditation Program (DIACAP). We will continue to obtain the appropriate security certifications and conduct audits to demonstrate the security of our infrastructure and services. For more information on risk and compliance activities in the AWS cloud, consult the Amazon Web Services: Risk and Compliance whitepaper.

Logical access for remote administration and software deployment to In Case of Crisis instances is restricted to our team of Systems/Network Engineers. Remote access for administrators is protected with multi-factor authentication (username/password combination and a software token).

In Case of Crisis stores its database in a secure instance of Microsoft SQL Server within Microsoft Azure hosting services with restricted access to information-only permitted by approved IP addresses. This database resides in the South Central US.

➡ **Additional Information:** These are the same data centers that run many of the world's largest online services. These datacenters are designed and constructed with stringent levels of physical security and access control, power redundancy and efficiency, environmental control, and recoverability capabilities. The physical facilities have achieved broad industry compliance, including ISO 27001 and SOC / SSAE 16 / SAS 70 Type II and within the United States, FISMA certification. To ensure recoverability of the Windows Azure platform core software components, Microsoft has established an Enterprise Business Continuity Program based on Disaster Recovery Institute International (DRII) Professional Practice Statements and Business Continuity Institute (BCI) Good Practice Guidelines. This program also aligns to FISMA and ISO27001 Continuity Control requirements. As part of this methodology, recovery exercises are performed on a regular basis simulating disaster recovery scenarios. In the rare event that a system failure does occur, Microsoft uses an aggressive, root cause analysis process to deeply understand the cause. Implementation of improvements learned from outages is a top priority for the engineering organization. In addition, Microsoft provides post-mortems for every customer impacting incident upon request. For more information, you can consult their security website here: Azure Security.

Database access is restricted to our team of database administrators. Remote administration is limited to sites specified within a set of rules within SQL Azure. All communications between the database and web server are encrypted. The SQL Azure data store is encrypted at rest using Microsoft Azure TDE, which uses AES-256 bit encryption.

ARCHITECTURE OVERVIEW

In Case of Crisis works using the following components:

- **Mobile device (iOS, Android, Windows, Kindle Fire)**
- **Web server/Application Server**
- **Database**

The process of obtaining the In Case Of Crisis app and downloading your plans is as follows:

- **The mobile device downloads the appropriate application (In Case of Crisis) from the App Store/Google Play/Windows Store/Amazon.**
- **The application then presents the user with the option to add a plan to the application.**
- **The application requests the plan from the web server**
- **The web server processes the request and pulls the plan from the database over the encrypted secure channel.**
- **The web server makes the plan available to the application and the application downloads the plan to the mobile device.**
- **The application on the mobile device stores the info within the local application data store and displays the plan information for the user.**

Again, all communications between the mobile device application and the web server are TLS 1.2 encrypted.

The In Case of Crisis database is encrypted at rest and a real time replication of the encrypted data is performed to a secondary database allowing a point in time restore within the last 35 days.

Only RockDove Solutions Mobile App and Support Team have access, security is strictly enforced through Firewall, IP filtering, and multi-Factor Authentication.

However, database access from the In Case of Crisis mobile application is not business critical. The application is stored within the users' phone and all authorized plans are stored within the application. Therefore, any disruption of service will only be noticeable by users who have yet to download the application and retrieve their plans.

In Case Of Crisis monitors the health and performance of all systems through cloud provider and onsite monitoring systems that notify our administrators immediately in the event of an outage or performance issue.

CLOUD-BASED HOSTING SERVICES

Link to Microsoft Azure's SOC 1/SSAE 16/ISAE 3402 and SOC 2 Attestations.
http://azure.microsoft.com/en-us/support/trust-center/compliance/soc-1/

Link to AWS SOC Report FAQs
https://aws.amazon.com/compliance/soc-faqs/

Link to request an AWS business representative who may provide the reports
https://aws.amazon.com/compliance/contact/

Link to AWS's SOC 3 report
https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

REVISON HISTORY

REVISION DATE	VERSION	COMMENTS
05/16/2016	1.0	Document Created.
06/14/2018	1.1	Updated SHA-2 as min encryption standard. Added Windows store as supported OS. Clarified two-factor authentication.
08/30/2019	3.0	Reviewed for accuracy and completeness