Scope 5 Security Policy and Breach Protocol

Updated September, 2013

Our Commitment

At Scope 5 we recognize that our customers trust us with their data and that we have a huge responsibility to keep that data secure. In the following paragraphs, we describe our security mechanisms and the protocol that we follow in case of a suspected breach.

Security Mechanisms

The Scope 5 application and all customer data are hosted 'in the cloud'. As such, there are several points at which customer data must be protected. We employ industry standard security mechanisms at each of these points, as follows:

- **Protection of databases from unauthorized electronic or physical access** – Customer data is stored in databases that are hosted on *Amazon Web Services* (AWS)[1], by *Heroku*, a *Salesforce* company. As such, we benefit from the state-of-the-art security mechanisms provided by these organizations. Further details on these are available here: https://www.heroku.com/policy/security
- **Protection from unauthorized application level access to customer data** – Our application allows authorized administrators electronic access to their data using encrypted passwords (passwords are never stored in clear text). The same mechanism prevents unauthorized application access to customer data.
- **Protection from network snooping** – We encrypt all communications between user terminals/computers and hosting servers using *Secure Sockets Layer* (SSL).
- **Protection of data by Scope 5 employees** – Scope 5 has strict protocols in place regarding employee handling of customer data. All Scope 5 employees sign agreements to abide by these.

Breach Protocol

We rely on two mechanisms to discover breaches:

1. Notification by our platform providers (Heroku, Salesforce or Amazon)
2. Routine inspections of application access conducted by our developers

In the event of a breach, we:

1. Immediately take any affected database(s) and application software offline.
2. Work with our legal team at Perkins Coie to identify and fulfill any legal obligations related to the breach.
3. Notify our customers that a breach has been detected.
4. Work with our platform providers and their forensics teams to understand the extent and nature of the breach.
5. Document everything known about the breach.

Feedback and Vulnerability Reporting

We take our responsibility for the security of our customer's data very seriously. We welcome any input you may have on our security mechanisms and encourage you to report any suspected vulnerabilities immediately to security@scope5.com.

Additional Documentation

Additional documentation regarding specific Scope 5 security protocols is available by request.

---

[1] http://www.informationweek.com/security/management/5-ways-amazon-web-services-protects-clou/240008405