Data security and architecture at Scoop

Scoop for Hybrid Work

What is Scoop?
Scoop partners with businesses to help them operate a hybrid remote and in-office workforce while maximizing safety, productivity, and engagement.

About the Scoop platform
Scoop’s platform includes mobile apps and desktop extensions for employees and a web-based Dashboard for customer administrators.

Our data security and architecture

Data collection and communication
All data provided by employees or administrators via the Scoop mobile apps, desktop extensions, and Dashboard is encrypted in transit between the public internet and Scoop’s networks in AWS (TLS 1.2). Data is also encrypted at rest using AWS-managed keys. User passwords are encrypted (salted and hashed) using modern encryption libraries, and multi-factor authentication is required for every account. Data submitted by clients is heavily validated for correctness, and system logs strive to never include sensitive information.

Infrastructure and backups
Scoop uses Amazon Web Services to host the majority of its cloud infrastructure, including its databases and API servers. Scoop uses AWS-provided backup systems which are heavily tested and reliable. We do not store data in systems not managed by AWS.

Data access controls
The Scoop team seeks to restrict access to all user information to only those on the team who require it in order to help provide the Scoop service.

Data guidelines, team protocols, and monitoring are evaluated in concert with Scoop’s legal counsel and maintained to the best of our knowledge.

Physical security
The Scoop office is secured by a keycard system. No data is stored on premise, and all employee devices are secured and remotely accessible.

Network security
Scoop follows networking best practices, and follows the principle of least privilege when it comes to firewall rules. We rely on code-managed configuration of AWS’s Virtual Private Cloud. We encrypt traffic in transit, and don’t grant any special privileges to our office network.

Monitoring and logging
Relying on sophisticated 3rd-party services, Scoop logs and monitors infrastructure events, application events, and access. This enables historic audit logging as well as providing threshold and rate alerting to indicate both performance and security events.

SOC-2 Type II and CCPA compliant
Scoop is SOC-2 Type II certified and fully CCPA compliant. All user account information is available for download or deletion upon request.
Information collection & handling

What information does Scoop collect from employees via mobile apps or desktop extensions?
Scoop collects the following basic information to be able to facilitate our service for employees. Only bold information is required by Scoop.

<table>
<thead>
<tr>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identity</td>
</tr>
<tr>
<td>Phone number</td>
<td>Multi-factor security</td>
</tr>
<tr>
<td>Work email address</td>
<td>Account verification</td>
</tr>
<tr>
<td>Vaccination status &amp; documentation</td>
<td>Workplace safety</td>
</tr>
<tr>
<td>Physical location*</td>
<td>Attendance verification</td>
</tr>
</tbody>
</table>

| *Physical location is optionally enabled to automate workplace check-ins. Storage of location data is limited to the single location point that verifies check-in. No other location data is stored by Scoop and location information is never provided to administrators. |

What information does Scoop collect from administrators via the Scoop Dashboard?
Scoop collects the following basic information to be able to facilitate our service for administrators. Only bold information is required by Scoop.

<table>
<thead>
<tr>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee roster</td>
<td>Account creation</td>
</tr>
</tbody>
</table>

What information does Scoop provide to administrators via the Scoop Dashboard?
Scoop provides the following information to administrators in the Scoop dashboard:

<table>
<thead>
<tr>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workplace attendance log</td>
<td>Attendance visibility</td>
</tr>
<tr>
<td>Vaccination status &amp; documentation</td>
<td>Workplace safety</td>
</tr>
</tbody>
</table>

Administrator access controls

Who can access the Scoop dashboard?
Scoop Dashboard access is restricted to administrators that are designated by a Scoop customer. All administrator accounts must be authenticated and access records are logged.

Health information and vaccination records

How is vaccination information stored and accessed?
All vaccination documentation provided by employees is encrypted in transit between the public internet and Scoop’s networks and AWS, and encrypted at rest using AWS-managed keys and stored securely in AWS S3. Links utilized to view documentation (e.g. for review and verification) are short-lived and expire to prevent the documentation link from being discoverable/shareable. Only Dashboard administrators are able to access the vaccination documentation, and Scoop employee access is limited in accordance with the “Data access controls” outlined above.

Vaccination documentation can be deleted or downloaded upon request, in accordance with CCPA requirements. As a 3rd party software provider, Scoop itself is not subject to HIPAA requirements. Nonetheless, Scoop has implemented every industry-leading protocol to protect access to sensitive vaccination information.