

Safety In Motion, Inc. (“SIM Inc.”) Privacy Policy

Updated: August 5, 2016

This privacy policy is here to help you understand what information we collect at SIM Inc., how we use it, and what choices you have. When we talk about SIM Inc. in this policy, we are talking about Safety In Motion, the company, SIM-Works™, the downloadable application, and websites that are available for use via a web browser or applications specific to your desktop or mobile device.

This policy describes how SIM Inc. treats your information, not how other organizations treat your information. If you are using SIM Inc. in a workplace or on a device or account issued to you by your employer or another organization, that company or organization likely has its own policies regarding storage, access, modification, deletion, and retention of communications and content which may apply to your use of SIM Inc.. Content that would otherwise be considered private to you or to a limited group of people may, in some cases, be accessible by your Consultant or administrator. Please check with your employer, Consultant or administrator about the policies it has in place regarding your communications and related content on SIM Inc.. More on this below.

In this policy we talk about various roles within an account and the privileges that come with each. It's helpful to understand these roles and the relationships between them. Here's the breakdown: Consultant>Administrator>SIM-tech™. Consultants have the most control over their account on SIM Inc., followed by Administrators. The person who establishes the account is considered the primary owner with the most control over the account (which is why it's not a good idea for this person to be a contractor or temp employee). Accounts can have more than one administrator. Administrator responsibilities can be transferred to another member after the account is created (see prior note about temp workers and flaky people). All Consultants are administrators, and all consultants and administrators are also SIM-techs™.

Information we collect and receive

We collect different kinds of information. Some of it is personally identifiable and some is non-identifying or aggregated. Here are the types of information we collect or receive:

- **Account information.** When an account is created, you may have 1+ administrators. Administrators can create SIM-techs™, select which techniques are available and run reports. Additionally, they will have access to the mobile app.
- **Profile information.** The only information we require to create your SIM Inc. account is an email address, username, and password. Any information you add to your profile is visible to other administrators and consultants within your account as described on your profile management page.
- **Log data.** When you use SIM Inc., our servers automatically record information, including information that your browser sends whenever you visit a website or your mobile app sends when you're using it. This log data may include your Internet Protocol



address, the address of the web page you visited before coming to SIM Inc., your browser type and settings, the date and time of your request, information about your browser configuration and plug-ins, language preferences, and cookie data. Log data does not contain message content and is not routinely deleted.

- **Device information.** In addition to log data, we may also collect information about the device you're using SIM Inc. on, including what type of device it is, what operating system you're using, device settings, unique device identifiers, and crash data. Whether we collect some or all of this information often depends on what type of device you're using and its settings.
- **SIM Inc. usage information.** This is information about which accounts, users, features, and content, you interact with within SIM Inc. and what integrations with related services you use.
- **Communication content that you send and receive within SIM Inc..** This includes:
 - The message content itself. This content can include messages, pictures, files and video among other types of files.
 - When messages or files were sent and by whom, when or if they were seen by you, and where you received them (in a channel or direct message, for example).
- **Information from partners or other 3rd parties.** SIM Inc. may receive information from partners or others that we could use to make our own information better or more useful. This might be aggregate level information about which IP addresses go with which zip codes or it might be more specific information about how well an online marketing or email campaign performed.

Our Cookie Policy

SIM Inc. uses cookies, or similar technologies like single-pixel gifs and web beacons, to record log data. We use both session-based and persistent cookies.

Cookies are small text files sent by us to your computer and from your computer to us, each time you visit our website. They are unique to your SIM Inc. account or your browser. Session-based cookies last only while your browser is open and are automatically deleted when you close your browser. Persistent cookies last until you or your browser delete them or until they expire.

Some cookies are associated with your SIM Inc. account and personal information in order to remember that you are logged in and which account you are logged into. Other cookies are not tied to your SIM Inc. account but are unique and allow us to do site analytics and customization, among other similar things. If you access SIM Inc. through your browser, you can manage your cookie settings there but if you disable all cookies you may not be able to use SIM Inc.



SIM Inc. sets and accesses our own cookies on our company-owned domains. In addition, we use 3rd parties like Google Analytics for website analytics. You may opt-out of third party cookies from [Google Analytics](#) on its respective website. We do not currently recognize or respond to browser-initiated Do Not Track signals as there is no consistent industry standard for compliance.

How we use your information

We use your information for the following:

- **Providing the SIM Inc. service.** We use information you provide to authenticate you and deliver message content to you and from you
- **Understanding and improving our products.** To make the product better we have to understand how users are using it. We have a fair bit of data about usage and we intend to use it many different ways to improve our products, including research. This policy is not intended to place any limits on what we do with usage data that is aggregated or de-identified so it is no longer tied to a SIM Inc. user.
- **Investigating and preventing bad stuff from happening.** We work hard to keep SIM Inc. secure and to prevent abuse and fraud.
- **Communicating with you**
 - **Solving your problems and responding to your requests.** If you contact us with a problem or question, we will use your information to respond to that request and address your problems or concerns.
 - **In-product communications.** We may use the information you provide to contact you through SIM Inc. using in-product messaging tools. For example, if, after, a few weeks of using SIM Inc. we notice that your notification setting is set to notify you of all messages, we may send you a SIM Inc. message that suggests you change this in case you are getting too many notifications. This is just one example of how we use information about your usage of the product to make suggestions to you.
 - **Email messages.** We may send you service and administrative emails, such as when we notice that you are nearing a message or integration limit. We may also contact you to inform you about changes in our services, our service offerings and important service related notices, such as changes to this policy or security and fraud notices. These messages are considered part of the service and you may not opt-out of them. In addition, we sometimes send emails to SIM Inc. users about new product features or other news about SIM Inc.. You can opt-out of these at any time.



Choices for Consultants and Administrators

- Consultants and Administrators have the ability to manage and change most of the administrative settings, including message retention settings, and can modify which techniques are available. Administrators can also deactivate user roles within their account.

Other Choices

- The browser you use may provide you with the ability to control cookies or other types of local data storage.
- Your mobile device may provide you with choices around how and whether location or other data is shared with us.
- SIM Inc. does not control these choices, or default settings, which are offered by makers of your browser or mobile device.

Sharing and Disclosure

There are times when communications and related content and other user information may be shared by SIM Inc.. This section discusses only how SIM Inc. may share user information. Organizations that use SIM Inc. may have their own policies for sharing and disclosure of information they can access through SIM Inc.. SIM Inc. may share information:

- **With consent, to comply with legal process, or to protect SIM Inc. and our users.** When we have your consent or if we believe that disclosure is reasonably necessary to comply with a law, regulation or legal request; to protect the safety, rights, or property of the public, any person, or SIM Inc.; or to detect, prevent, or otherwise address fraud, security or technical issues. If we receive a law enforcement or other third party request for information we will provide prior notice to the subject of the request where we are legally permitted to do so.
- **With third party service providers and agents.** We may employ third party companies or individuals to process personal information on our behalf based on our instructions and in compliance with this Privacy Policy. For example, we may share data with a security consultant to help us get better at preventing unauthorized access or with an email vendor to send messages on our behalf. We may also share data with hosting providers, payment processors, marketing vendors, and other consultants who work on our behalf.



- **About you with your company or Administrator(s).**
 - We may share your email address with your organization. If the email address under which you've registered your account belongs to or is controlled by an organization (to be clear, we're not talking about free web-based email providers like Gmail, Hotmail or Yahoo! Mail) we may disclose that email address and to that organization in order to help it understand who associated with that organization uses SIM Inc., and to assist the organization with its enterprise accounts. Please do not use a work email address for our services unless you are authorized to do so, and are therefore comfortable with this kind of sharing.
 - In addition, there may be times when you contact SIM Inc. to help resolve an issue specific to your company. In order to help resolve the issue, we may need to share your concern with your administrator. When possible, we will try to mask or remove any identifying information before sharing these communications.
 - As described above in the Message Retention Settings and Export Option section, Consultants and Administrators have certain rights to export their company's data.
 - If we engage in a merger, acquisition, bankruptcy, dissolution, reorganization, sale of some or all of SIM Inc.'s assets financing, acquisition of all or a portion of our business, or similar transaction or proceeding that involves the transfer of the information described in this Privacy Policy.
- **For Business and Research Purposes.**
 - We may also share aggregated or de-identified information with our partners or others for business or research purposes. For example, we may tell a prospective SIM Inc. customer the average number of observations submitted in a day or may partner with research firm or academics to explore interesting questions about workplace communications. Again, this policy is not intended to prohibit the disclosure and use of aggregated or de-identified data.

Security

SIM Inc. takes reasonable steps to protect information you provide to us as part of your use of the SIM Inc. service from loss, misuse, and unauthorized access or disclosure. These steps take into account the sensitivity of the information we collect, process and store and the current state of technology. When you enter sensitive information (such as sign-in credentials) we encrypt the transmission of that information using secure socket layer technology (SSL). We follow generally accepted standards to protect the personal data submitted to us, both during transmission and once we receive it. However, no electronic or email transmission or digital storage mechanism is ever fully secure or error free.



Changes to this Privacy Policy

We may change this policy from time to time, and if we do we'll post any changes on this page. If you continue to use SIM Inc. after those changes are in effect, you agree to the revised policy. If the changes are material, we may provide more prominent notice or seek your consent to the new policy.

EU Safe Harbor

SIM Inc. complies with the U.S. - E.U. Safe Harbor framework and the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. SIM Inc. has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement.

Contacting SIM Inc.

Please also feel free to contact us if you have any questions about SIM Inc.'s Privacy Policy or practices. You may contact us at www.SafetyInMotion.com or at our mailing address below:

Safety In Motion, Inc.
610 SW Broadway, Suite 310
Portland, OR 97239
USA

