



# RecoveryPlanner.com Privacy Policy

---

*Effective as of 8/19/2009*

## Overview

In order to operate the RecoveryPlanner.com website and the RecoveryPlanner.com Software as a Service ("SaaS"), RecoveryPlanner.com, Inc. ("RP" or "we") may ask you to provide information about yourself and ways you might be contacted. This Privacy Policy describes the information we collect and how we use that information.

RP takes the privacy of your personal information very seriously and will use your information only in accordance with the terms of this Privacy Policy. We will not sell or rent your personally identifiable information or a list of our customers to third parties. This Privacy Policy applies to both the RP website and the RP SaaS.

Any information you provide will be treated in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "EU Data Protection Directive"), and any implementing and/or amending legislation as may be adopted in EU Member States from time to time.

This privacy statement complies with the Safe Harbor framework under the EU Data Protection Directive. In addition, RP self-certifies compliance with the Safe Harbor framework to the U.S. Department of Commerce.

If you have questions or concerns regarding this Privacy Policy, you may contact RP via the Contact Information at the end of this document.

## Information We Collect

There are three inquiry forms on the RP website:

Demo Request – <http://recoveryplanner.com/DemoRequest/default.asp>

Partner Registration – <http://recoveryplanner.com/PartnerRegistration/default.asp>

Contact – <http://www.recoveryplanner.com/ContactForm/default.asp>

All three require input of Name, Company, Phone and Email Address. Optional street address information is also requested.

In addition to these forms, RP may gather data via other forms from prospective clients that will enable us to address their specific needs in a more targeted manner. This data may include industry segment, company size, current status of their business continuity efforts, etc.

The RP SaaS collects company personnel information including name and one or more specific contact methods so that people can be reached in the event a client activates a business continuity plan. This contact information can include physical street addresses, phone/cell/pager numbers, email addresses and IM addresses. It is up to individual client company policy to determine what personal information is to be provided by their employees. The RP SaaS application only stores this information for use by authorized individuals within a given client company and RP in no way uses this information for its own purposes.

## Cookies

When you interact with the RP SaaS we strive to make that experience easy and effective. To this end, we utilize cookies when possible with our application. Cookies are files that web browsers place on a computer's hard drive and are used subsequently by the web application that put them there to know what data was saved in the cookie. Cookies can be set to either expire at the end of your browser session (session cookies) or to remain until some expiration date in the future (persistent cookies).

When you login to the RP SaaS, you have an option to save your Client ID as a cookie. If you choose to do this, our web application server sends a persistent cookie to your browser (in this case, to tell us what Client ID you will be using each time you login). If your web browser is configured so that it will not accept cookies, you will need to enter the Client ID each time you attempt to login.

The RP SaaS application also attempts to maintain your unique user session by means of session cookies. Web applications are inherently stateless – there is no connection that is maintained between the client browser and the server application. Each time a user clicks on a link or a button in our application, data is sent back to our server, processed by our application and a response page is sent back to the user's browser. The way our application knows which user is making which request and where they are in the application is by storing data in variables within the user session on the application server, and a session ID is used to identify the unique session. This session ID is stored in a session cookie if your web browser is configured to accept cookies. If not, the session ID is automatically sent via the URL.

All cookies used by the RP SaaS application are encrypted via Secure Socket Layer (SSL) technology to ensure security as this data is transmitted between the application server and your browser.

## Server Logs

Web servers maintain log files that show each request and response processed by the server. These log entries contain data including the URL requested and the IP address of the machine making the request. Both the RP SaaS and the RP website store this log information and we use it for the purposes of

analyzing usage and making sure that no requests are being made from suspect locations. None of this data identifies unique individuals and it is only used for internal security purposes.

## **Auditing**

The ability to audit activity within the business continuity planning process is an important aspect of this function. The RP SaaS application stores information such as when individuals login and logout of the application, who made specific changes to a plan and when, who approved changes and when, etc. In addition, all information related to the execution of a specific plan is tracked for audit purposes. This information is accessible to authorized individuals within a given client organization and is not otherwise made available to users outside of that organization.

## **How We Use Collected Information**

Information collected from the RP website is only used to facilitate the dialog between RP and either current or prospective clients. This information is not shared with outside entities unless otherwise required by law.

## **Security**

Both the RP website and the RP SaaS have security measures in place to help protect against the loss, misuse, and alteration of the data under our control. When our website or SaaS is accessed, Secure Socket Layer (SSL) technology protects information using both server authentication and data encryption to help ensure that data is safe, secure, and available only to you. RP also implements an advanced security method based on dynamic data and encoded session identifications, and hosts both the website and SaaS in secure server environments that use firewalls and other advanced technology to prevent interference or access from outside intruders. Finally, RP provides unique user names and passwords that must be entered each time a client logs on to the SaaS. These safeguards help prevent unauthorized access, maintain data accuracy and ensure the appropriate use of data.

## **Opt-Out Policy**

RP offers its clients and prospects a means to choose how we may use information provided. If, at any time after registering for information or ordering the SaaS, you change your mind about receiving information from us, send us a request specifying your new choice via the Contact Information at the end of this document.

## **Accessing and Changing Your Information**

You can review the personal information you provided us and make any desired changes to such information, at any time by logging in to your account on the RP SaaS or by contacting us directly via the Contact Information at the end of this document.

## **Contact Information**

If you have any questions about this privacy statement, RP's information practices, or your dealings with RP, you can contact us via email at [support@recoveryplanner.com](mailto:support@recoveryplanner.com) or call our Help Desk at 203-455-9990 Monday through Friday between the hours of 9am and 5pm ET, or write us at [RecoveryPlanner.com](http://RecoveryPlanner.com), Inc., 101 Merritt Blvd, Trumbull, CT 06611.