About *courtbinder.com*

Overview

The *courtbinder.com* webapp is an online service which seeks to assist litigators to quickly prepare document collections for court and related client work.

It has been developed by an Australian software firm, Soferio Pty Limited (ABN 26 156 065 833). Tamir Maltz, a lawyer (counsel) based on Sydney, is a director of the firm and involved in the operation and development of the service.

Pricing

Courtbinder.com was launched in mid-2017, and is **freely** available at present while customer feedback is collected. It will then become a paid product.

Infrastructure providers

Secured by PayPal powered by amazon web services HEROKU SendGrid

Information Security

All documents are stored on Australian-based servers (deleted on a 24 hour cycle) on Amazon.com Inc’s secure AWS Platform. You can read about Amazon's security systems here.

The *courtbinder.com* web-site is hosted by a US-based commercial PAAS provider, namely *Heroku* (*courtbinder.com* is not otherwise affiliated with or otherwise sponsored by Heroku). You can read about Heroku's high-grade security systems, policies, and physical infrastructure here.

Payments are processed exclusively by Paypal, and you can read about Paypal's security systems here.

Email is sent solely by Sendgrid, using opportunistic TLS to encrypt email transmissions at the highest available encryption level from the receiving mail server.

Security Policy and Practices

In addition, *courtbinder.com* utilises its own web-application security technologies and processes, including the following, to fortify your data against unlawful intrusions:

- encryption in transit, using the HTTPS protocol and strict transport security;
- emails are sent at the highest available encryption using opportunistic TLS (by Sendgrid);
- use of (client-held) encrypted tokens to secure binders;

- logging and monitoring of suspicious alerts;
- throttling of requests;
- limited access to the files;
- REST-based authentication controls using encrypted tokens.

Bug reports

Subject to the acceptable use policy, and the absence of any publication prior to consideration and confirmed mitigation by Soferio Pty Limited, and all applicable laws, any security reports by full-time professional security researchers (who are wholly unaffiliated with competitors of the service) may be sent to info@soferio.com, and will (in Soferio Pty Limited's absolute discretion) be considered for inclusion in the security-researcher 'hall of fame' (currently no members).

It is difficult to provide a definitive list of bugs that will qualify for the 'hall of fame': any bug that substantially affects the confidentiality or integrity of user data is likely to be in scope for the program. Common examples include cross-site scripting and request forgery, as well as flaws in authentication or command injections.

The following attacks are definitely excluded from any inclusion in the hall-of-fame, and will be considered to be breaches of the law: attacks against underlying service providers (including Heroku), social engineering attacks or any misleading direct contact with employees or agents operating the Service, attacks by parties affiliated with competitors of the service, attacks on physical facilities, flaws present only when using out-of-date browsers, attacks undertaken by penetration testers (or security consultants) employed by us, attacks targeting any other user's account or data (i.e. other than your own account or your own test data), brute force or DoS attacks, or any attack which disrupts the operation of the Service for other users.