OrangeBoy, Inc.
Data Use and Security

OrangeBoy created Savannah to help public libraries understand the nature, rhythm, and cost of their customers' experiences. We did so with three paramount beliefs. Public libraries must:

- Understand the customer experience to effectively meet the needs of their communities;
- Stand accountable to their communities who entrust limited financial resources to them; and
- Ensure their long-term viability.

We do this in the spirit of The Golden Rule, treating our clients as we would wish to be served ourselves. This means we forthrightly:

- Communicate the data required to effectively employ Savannah;
- Explain how our services use that data and the steps we take to protect it; and
- Allow libraries to choose what data they employ and how they employ it.

This document is meant to explain each of those three points.

As you will see, in almost all respects the questions of what data we use and how we use it are up to you. Our aim is to provide you with a set of tools you can use to help accomplish your goals and improve your operations. We take great pride in making sure that our tools are secure by design, and we will always maintain a high level of security over your data. But security is a holistic matter and must be considered the responsibility of all actors in the system. To that end, we hope this document will help you understand not only the steps that we have taken to protect your data, but also the places where that protection depends on your own internal processes and security measures.

If, after reading this document, you still have questions about how we treat your data, please ask. We welcome the opportunity to discuss these matters with you, and we hope to regularly update this document to address frequently asked questions.

Data Use and Ownership

We recognize that you remain the owner of your data, even when we are hosting it for you, and we take great pains to protect your information from public disclosure. We anonymize or pseudonymize your data wherever possible. We use secure protocols for communicating and transferring customer-related data, we hold and store that data in secure databases, and we regularly monitor our systems for vulnerabilities and attacks.

We do not and will not sell your information to third parties or allow advertisers to use it to try to sell you or your patrons goods or services. Nor will we release client data to a governmental body or law enforcement agency except as required by law—and even so, we strive to give our clients prompt notice of any such requests so that they can help determine the appropriate response.

In addition, we endeavor to give you control over the data that is put into our system in the first place. For the most part, the types of data that we use are up to you. We rely on our clients to upload data to us, though we are of course available to help you through the upload process, and even to automate it where possible. If you are not comfortable with certain types of data being used in Savannah, we will work with you to ensure that that data is not uploaded or used—though of course, certain features often need certain types of data to function, and we cannot ensure that all functionality will work with all configurations of data. For more information about the pieces of data commonly uploaded by our clients, please see our "Data Requirements" document.

In no case do we seek or use specific details about the items your patrons check out of your library. We can, however, keep track of the general *type* of items that patrons checked out—a children's book, A/V material, or an audiobook, for instance. We use this data to group patrons into "clusters" based on their specific library usage behaviors, which helps our clients gain insight into their patrons' usage of library resources and potential ways to increase engagement and better allocate scarce resources. Similarly, we can incorporate public demographic and address information into our analysis to uncover patterns in cardholder populations (as well as to identify potential new cardholders and other growth opportunities). But in any event, it will always be your choice whether—and if so, how—to utilize this data.

As allowed by law and our contracts with clients, we may derive aggregated, anonymous statistical insights about the industry from data submitted by our clients. These industry insights will not include any personally identifiable information, will not identify any particular OrangeBoy client, and will be used only in the aggregate to help clients see how their data metrics compare to those of similarly situated libraries.

System Security

We host our Savannah system on Microsoft Azure because we believe that Microsoft brings a level of expertise and resources to their hosting practices that few other entities can provide. We can therefore leverage Microsoft's efforts to ensure that Savannah remains reliably available and highly secure regardless of how much traffic we are supporting. Microsoft has put in place numerous redundancies, not only in hardware and software, but also in the physical location of their datacenters, to ensure that they can provide reliable service even in the face of serious threats. For more about Azure's security practices, see https://docs.microsoft.com/en-us/azure/security/.

We maintain separate development and production environments for Savannah, as well as a code repository and standard quality assurance procedures, to ensure that untested code is not used by our customers. Similarly, we maintain separate databases for each customer to ensure that each customer's data is logically separated from that of other customers, providing an additional layer of security. Moreover, we do not use production data for testing, except as required to resolve an issue that a client has reported to us.

We encrypt client data at all times, including when in transit, at rest, and when backed up. We require our employees to follow secure practices in their day-to-day operations, including using secure means whenever they need to transfer client data, in addition to their contractually required nondisclosure obligations. We use industry-standard security and protection software on all company computers, which are regularly scanned and patched as necessary. Each employee has a separate user account, with need-to-know authorizations tailored to their particular role. Employee passwords must meet strict requirements, and employee accounts failing those requirements or otherwise showing signs of disuse are disabled. We work with an employment screening vendor to complete background checks on all new hires. When an employee leaves OrangeBoy, we terminate their accounts and access the same day, and we regularly review all accounts' access privileges to ensure that we are not granting broader access than is currently necessary.

Along with Microsoft Azure, we use SendGrid to help us send messages to your cardholders. And we use both SurveyGizmo and SendGrid to help send and collect surveys to existing or potential cardholders. We have carefully screened these providers to ensure that they also take appropriate steps to maintain the security and confidentiality of any data that they handle. By default, our message provider uses special URLs and adds a small image to the end of email messages so that we can give you statistics on message open rates and click-through rates. We can turn off this setting for clients who do not want it. In any event, SurveyGizmo and SendGrid will not receive any information whatsoever unless you choose to send a message or survey, and even then they will receive only the information necessary to do their jobs—in no case will they have access to our clients' raw data.

In addition, our clients often ask us to work with other vendors—for instance, to upload data that is currently stored with e-book providers or ILSs. When we work with these vendors, we do what we can to ensure that they use secure practices. But because these third parties' relationships are with the library and not us, we cannot always control their security practices. In such cases, we have to rely on those third parties to ensure that safe practices are followed.

We rely on our clients to follow safe practices as well. For instance, we ask that our clients ensure that only trusted users are given access to our services, that proper password safety principles are enforced, and that we are informed promptly whenever a user's access should be terminated (such as when an employee quits or no longer needs access). We further rely on our clients to communicate with their cardholders, informing them of how their data may be used and obtaining

any necessary permissions. And, of course, we rely on our clients to decide in the first place just what data to use and how to use it. Again, our goal is to provide our clients with powerful, well-designed tools, but ensuring that those tools are used appropriately is everyone's responsibility.

Finally, we know that not all security incidents can be prevented, regardless of the security precautions put in place. For that reason, we have implemented an incident response plan to ensure that if the worst happens, our team will be able to respond immediately to minimize the chance of disruption to our clients' operations. Employees must report any suspected security issue to supervisors, who then organize the team responsible for investigating, containing, and recovering from any incident. We are committed to transparency, and so we will notify you as soon as possible if we determine that a security breach affected your data or allowed unauthorized access to it in any way. We further commit to working with affected clients to provide any necessary information, help determine their own responses, and take any remedial action necessary.

Client Control and Deletion of Data

Our clients always retain ultimate control over their data. On written request, we will delete all or part of a client's data—anything from a particular cardholder's records to the entirety of the data uploaded to Savannah. Once this data is deleted, of course, we can no longer recover it, and deleted data may no longer show up in client reports.

We can also provide exports of client data on request, though the exact format and structure of our export files will depend to some extent on the structure of our databases and the technological capabilities associated with them.

* * *

We hope this document has answered any questions you have about how we use and protect your data. If you have any further questions, however, please just get in touch. We would be glad to speak with you about any of these matters.

Last revised August 11, 2023