SPEKTRIX PRIVACY AND SECURITY POLICY

1. SPEKTRIX TRUST COMMITMENT

Spektrix is committed to gaining and maintaining the trust of all our clients. As part of this commitment, Spektrix provides robust security and privacy procedures that carefully consider data protection across its platform and services, to ensure we maintain the confidentiality, integrity and availability of data submitted by our clients and their customers ("Customer Data").

2. SERVICES COVERED

This documentation supplements the agreement our clients have with Spektrix including the Spektrix Data Processing Addendum and describes the security and privacy related audits, certifications, technical and physical controls applicable to the Spektrix multi-tenant SaaS platform.

The "Client Interface" refers to the interface for our clients
via: https://system.spektrix.com/<client_id>/client

The "Customer Interface" refers to the IFrame integration that the client would host on their public facing website that allows customers to purchase tickets.

The "API" (or Application Programming Interface) refers to a set of subroutine definitions, protocols, and tools for secure programmatic access to the Spektrix platform.

3. DATA CONFIDENTIALITY

3.1. Data Encryption

Spektrix uses industry-standard encryption to protect Customer Data and communications during data transmissions from the Customer Interface, Client Interface and API on a client's or partner's network, to the Spektrix service, including Transport Layer Encryption (TLS) leveraging RSA certificates.

3.2. Sensitive Data

Spektrix does not store any credit card or payment information. There are options in the system to enter in free text (for notes against a customer for example) and the client is responsible for how it decides to make use of these fields.

3.3. Control of Data Processing

Spektrix has strict policies on accepting management or support requests. For example: the Spektrix support team will assist users with how to perform a password reset, but the user themselves will need to perform the actual actions (and therefore will have to have the necessary privileges to do so).

Similarly, for day-to-day support calls, the Spektrix team member will typically talk a user through how to perform actions for themselves as opposed to performing the actions for the user.

For situations where a change needs to be made by the Spektrix support team, these would have to be sent via our support centre, which involves authenticated access.

All user passwords are stored using a one-way salted hash.

Passwords are never logged.

Passwords must be a minimum of 8 characters in length and contain a combination of alphanumeric and non-alphanumeric characters. Repeated failed attempts to enter passwords will lock user accounts.

3.4. Certification

Spektrix conforms with the PCI-DSS standard for the handling of cardholder data and is audited annually as a PCI Level 1 provider.

Spektrix has a governance framework which is managed by the Chief Security Officer and is comprised of:

- A risk management plan and incident management plan which is tested at least annually; and
- Regular meetings within our infrastructure team to review security practices and procedures; and
- An information security policy which is regularly reviewed and updated; and
- Penetration Testing of the Spektrix application by a qualified third party, carried out annually, or whenever major architectural changes are made to the application.

3.5. Security Controls

Roles in the system allow differing levels of access ensuring users only have access to the areas of the system required.

The Spektrix system allows clients to limit where the client interface can be accessed from (by IP). In the event of access being required outside the client's network, Spektrix provides a mechanism for access from unknown IP addresses. This is done by a request being made for temporary access which can be granted by a user with administrative access for between 1 and 30 days, and which can be revoked at any time.

Various audit trails are made available in the Spektrix application:

- Full details of all changes made to customer records including before and after values of all fields that have been changed; and
- Full order history including time and user who performed every action and details of those actions; and
- Auditing of changes to other system objects, but not at the same level of detail as above due to less critical nature of the data.

3.6. Personnel Security

A minimum of two references are taken for every new staff member.

The number of staff members with access to the live infrastructure is kept to a minimum and criminal record checks are performed against all of these individuals.

Security training is provided for all staff members as part of their induction and repeated annually..

3.7. Operational Security

Various measures are in place to ensure operational security:

- Spektrix uses Cloudflare technologies to help mitigate web born security risks.
- Spektrix engages a qualified third party to perform annual external penetration testing.

- Access to the live environment is limited to just technical personnel who are fully trained and who have a need to access it, and is always through two-factor authentication.
- A patch management policy handling both "business as usual" patching on a regular schedule, as well as critical patches that could be deployed in a matter of hours across all systems depending on assessed risk.
- There is a formal change management process in place on the live system that involves risk assessment procedures and roll back plans.

3.8. Secure Development

All developers receive training in techniques for secure web application development, in particular around the Open Web Application Security Project's (OWASP) list of the top 10 most critical web app security risks.

All changes to code must be risk assessed by the developer and then code reviewed by at least one other developer.

Third party penetration tests will potentially be employed if particularly significant changes are being made to the operation/architecture of the application.

3.9. Analytics

Spektrix may track and analyse the usage of the Client Interface for purposes of user experience, by analysing trends, and tracking which features are used most often or need to be improved. No Customer Data consisting of personally identifiable information is contained in such derived data.

3.10. Third-Party Applications

Spektrix provides an API that a client, or a partner the client has an agreement with, may use for purposes such as transaction processing, data extraction and managing customer records. Spektrix provides the client with the ability to generate security keys to ensure that only permitted parties may use the API on a client's behalf. It is the responsibility of the client to ensure that agreements, policies, data security and privacy requirements are in place with any party accessing the API. Third party applications include, but are not limited to, payment service providers, email marketing platforms, data aggregators and web agencies.

4. DATA INTEGRITY

4.1. Architecture and Data Segregation

As a true multi-tenant and native cloud-based application, clients of Spektrix share a single application layer; however, behind this, each Spektrix client has their own database within our infrastructure that is separate from other client databases. The system has been engineered from the ground up with fail-safes in place to ensure that the application layer can only ever access the correct database depending on the user making the request.

4.2. Sub-Processors in Data Storage

Spektrix has entered into written agreements with sub-processors containing privacy, data protection and security obligations that provide industry standard levels of protection for their processing activities. A list of these sub-processors can be accessed via Spektrix Support Services. The key

providers that are involved in our supply chain are – Pulsant, Microsoft Azure, Loho, Cloudflare and AWS. Spektrix have contractual provisions in place with these providers to ensure appropriate security controls.

The Spektrix application is primarily located in Microsoft Azure data centres. The Microsoft Azure data centres where Spektrix is located are geographically dispersed within the EU, with geo replication across locations. Aspects of the infrastructure are also run in the AWS EU Ireland region. AWS and Microsoft Azure comply with key industry standards, including ISO/IEC 27001:2013 and NIST SP 800-53.

Microsoft designs, builds, and operates data centres in a way that strictly controls physical access to the areas where data is stored, with a layered approach to physical security, to reduce the risk of unauthorised users gaining physical access to data and the data centre resources. Data centres managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the data centre floor.

Upon a system's end-of-life, Microsoft operational personnel follow rigorous data handling and hardware disposal procedures to assure that hardware containing Spektrix data is not made available to untrusted parties. Microsoft use a secure erase approach for hard drives that support it. For hard drives that can't be wiped, they use a destruction process that destroys the drive and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. All Azure services use approved media storage and disposal management services.

4.3. User Authentication

Access to the client interface requires authentication via a username and password. Users of the system can be created, modified and deleted by users assigned to the role of Administrator.

5. AVAILABILITY

5.1. Incident Management

Spektrix would notify clients without undue delay of any unauthorised disclosure of their respective Customer Data.

Spektrix publishes system status information on its status page (https://status.spektrix.com/). Spektrix notifies customers of any significant system incidents via email and the Client Interface.

Spektrix has a formalised incident management plan, which is tested regularly via incident drills.

5.2. Reliability and Backup

Microsoft Azure ensures high availability through advanced monitoring and incident response, service support, and backup failover capability. The Microsoft Azure data centres where Spektrix is located are geographically dispersed within the EU, with geo replication across locations. This allows us to failover to the secondary data centre in the unlikely event of a disaster or large scale outage in the primary data centre. Data is backed up continuously to the secondary data centre within one second, so we have the ability to restore any of our clients' Spektrix systems to any point in time in the event of an issue.

5.3. Destruction of Data

As per Terms and Conditions, Spektrix may destroy or otherwise dispose of any of the Client's data in its possession unless Spektrix receives, no later than ten days after the effective date of the termination of this Agreement, a written request for the delivery to the Client of the then most recent back-up of the Client's data. Spektrix shall use reasonable commercial endeavours to deliver the back-up to the Client in an interchange format and within 30 days of its receipt of such a written request.

6. AMENDMENTS TO THIS POLICY

This policy will be regularly reviewed and updated from time-to-time by Spektrix to reflect any changes in legislation or in our methods or practices. The current version of the policy will be accessible via Spektrix Support Services.