info@eventoptions.co.za
www.eventoptions.co.za

eventoptions
the registration team

EVENT OPTIONS SECURITY POLICY

Event Options specializes in event RSVP and conference registration solutions. Owning hardware and software, we offer a flexible, pay-as-you-go pricing model using Evolve, a mobile-responsive RSVP and event check-in solution. At Event Options, we are dedicated to maintaining the security and confidentiality of our customers' data by adhering to data protection laws, including the Protection of Personal Information Act, 2013 (“POPIA”) and maintaining a culture of security awareness through employee training.

This security policy outlines the measures that we have implemented to protect your information while using our conference registration solutions and associated services. By choosing to use our services, you agree to comply with this security policy and trust us to protect your data.

1. Data Collection and Usage

We collect and use personal data, including but not limited to email addresses, phone numbers, names, organization information, and addresses, solely for the purpose of providing and developing our services. You agree to the collection and use of this information when registered to our service.

1.1. Data Collection

We collect your data through the following measures:

- Submission of forms on our websites or those provided by you.
- Posting comments or content on our social media pages or conference platform.
- Direct communication with us, where you provide information.

1.1.1. Data Collected by Cookies

We use Cookies along with other tracking technologies to analyze data and enhance our service. You have the option to set your browser to reject Cookies, but some features of our Service may not function properly without them.

1.2. Data Sharing and Access

We take commercially reasonable steps to protect your information. In addition, we also try our best to protect your personal information by using up-to-date technology and by being compliant under applicable law including the POPIA. To maintain these standards, the following guidelines must be adhered to regarding data sharing and access:

1.2.1. Approved Platforms for Data Sharing

All data sharing will be conducted exclusively through **Microsoft SharePoint** or **Evolve**, our secure registration platform.

1.2.2. Access Requirements

If you require access to specific data, it must be obtained either:

- ○ Through **Microsoft SharePoint**, where files are securely stored and managed.
- ○ By securely logging into **Evolve**, which provides direct access to the necessary data

1.2.3. Restrictions on Unauthorized Methods

- Data will **not** be shared through email, unsecured file-sharing platforms, or any other unauthorized methods.
- If you are unable to access SharePoint, your only alternative is to securely log in to Evolve.

1.4. Children's Privacy

Children under the age of 18 are not permitted to use our service. We do not gather personal information from children deliberately and if we come across such information, we will take appropriate action to remove it.

1.5. Your Choices, Rights, and Responsibilities

Event Options respects your ownership rights to your personal information.
You have the following rights as the owner:

- Your personally identifiable information may be transmitted to and processed in countries where our service providers are based. You consent to this transfer when you submit your information.

- At any time, you have the option to request clarification from us regarding the existence of any of your personal information in our possession.

- You have the right to request a copy of the personal information we have on record for you. We shall provide you with a copy of the information within a reasonable timeframe if we receive an authorized access request. You have the right to know the identity or categories of third parties to whom we have given your personal information. Such details will also be provided upon request.

- If you believe that any of the personal information, we have on record for you is incomplete, misleading, incorrect, or excessive, you have the right to have it corrected or deleted. In compliance with current data protection rules, we will review your request and make any required modifications or deletions.

2. Infrastructure and Hosting

Event Options relies on Amazon Web Services (AWS), a highly secure and renowned cloud service provider, to host our event registration solutions and associated services. AWS's robust and scalable infrastructure adheres to strict security standards, ensuring the utmost protection for our clients' data.

2.1. Access control

AWS employs multiple layers of security controls, including physical, network, and data security measures, within their data centers. Access controls and surveillance systems are in place to prevent unauthorized access.

1.2.2. Data Access

- **Event Options personnel** under strict contractual agreements, ensuring compliance with our security and confidentiality requirements.
- **Authorized users**, as determined and approved the client.

Unauthorized access or sharing of data is strictly prohibited.

2.2. Encryption

Data transmitted between clients and our servers, as well as data at rest within our databases, is encrypted using industry- standard protocols like Transport Layer Security (TLS) and Advanced Encryption Standard (AES).

Our software is hosted on Amazon RDS (Relational Database Service), a fully managed database service provided by Amazon Web Services (AWS). Amazon RDS offers robust security features to safeguard our data and ensure compliance with industry standards and regulations.

- Encryption at Rest: All data stored on our Amazon RDS instances is encrypted at rest. This ensures that even if unauthorized access to the underlying storage occurs, the data remains protected and inaccessible without proper decryption keys.

- Encryption in Transit: Data transferred between our application and the Amazon RDS instances is encrypted in transit using SSL (Secure Sockets Layer). This encryption mechanism prevents interception and tampering of data during transmission.

- Key Management: Amazon RDS utilizes AWS Key Management Service (KMS) for encryption key management. With KMS, we have full control over the creation, rotation, and management of encryption keys, ensuring secure key storage and access control.

- Compliance and Certifications: Amazon RDS complies with various industry standards and regulations, including PCI DSS, HIPAA, and GDPR. By hosting our software on Amazon RDS, we ensure that our data storage practices align with these compliance requirements.

- Data Privacy and Integrity: Amazon RDS provides features such as Transparent Data Encryption (TDE), which automatically encrypts and decrypts data as it is written to and read from storage. This maintains the privacy and integrity of our data without impacting application performance.

By leveraging Amazon RDS for our hosting infrastructure, we enhance the security posture of our software application, mitigating risks associated with data breaches and ensuring the confidentiality, integrity, and availability of our data assets.

2.3. Compliance

AWS is committed to data security and privacy via compliance with the ISO/IEC 27001 standards

2.4. Data Retention and Destruction

- Data will be retained for **30 days following the conclusion of an event** or until otherwise requested by the client.
- Upon the client's request, data will be securely destroyed in compliance with data protection regulations and organizational policies.

3. Information Security

The Event Options system is built using PHP Laravel framework and ensures information security via following methods:

3.1. Authentication and Authorization

Our robust and user-friendly authentication system with login throttling, CSRF protection, and password encryption, ensuring a secure and straightforward login experience. Additionally, our authorization system provides fine-grained access controls, granting access to specific parts of your application only to authorized users, and safeguarding sensitive data and limiting actions to approved individuals.

3.2. Encryption

At Event Options, we have simplified the process of securing sensitive information, such as user credentials to ensure the confidentiality and protection of valuable data by using an inhouse API to encrypt and decrypt data effortlessly.

3.3. Secure Validation and Error Handling

We have implemented safe validation steps to prevent our system from security attacks such as SQL injection and cross-site scripting (XSS). Additionally, our error handling system is designed to send accurate error notifications only to authorized users, reducing the danger of data leakage.

3.4. Secure Third-Party Applications

This security policy outlines the security measures we have established to protect your information as you utilize our conference registration systems and related services. By using our services, you agree to follow our security policy and trust us to protect your data.

3.5. Database Security

Our databases are highly secured to prevent unauthorized access and data breaches.

3.6. File Permissions

We maintain correct file permissions to restrict access to sensitive files and directories.

3.7. Updated SSL Certificates

We regularly update and maintain secure SSL certificates to encrypt data exchanged between clients and our servers.

3.8. Daily Backups

We perform daily backups to ensure data integrity and provide a safety net against potential data loss.

4. Incident Response Management

Event Options has established incident response procedures to handle security incidents effectively. The Incident Response Team will take appropriate actions to contain, mitigate, and recover from security incidents.

Clients and users will be promptly notified via email in the event of planned system maintenance or unexpected downtime. The notification will include the reason, estimated downtime duration, and updates until normal operations are restored.

5. Secure Development Practices

We follow a comprehensive Software Development Life Cycle (SDLC) methodology that governs the entire process of acquiring, developing, implementing, configuring, maintaining, modifying, and managing software components.

To ensure the integrity and security of application source code, we use a version management mechanism. Access to the source code repository is reviewed on a regular basis and restricted to authorized employees.

We have implemented a security-driven approach by conducting architecture reviews, open-source scans, and dynamic application testing to ensure secure development practices.

6. Security Awareness

Event Options is committed to fostering a culture of security awareness among our employees. We conduct regular security training and education programs to ensure that all staff members are knowledgeable about potential risks and best security practices.

7. Policy Updates

This Security Policy may be updated periodically to reflect changes in our security practices and legal requirements. We will notify clients of any significant changes via email or through a notice on our website.

8. Contact Information

If you have any questions or concerns regarding our security policy, please contact us at info@eventoptions.co.za.

This Security Policy outlines Event Options' commitment to maintaining a secure environment, protecting sensitive data, and responding effectively to security incidents. All employees and users are expected to adhere to this policy to ensure the highest level of security and data protection. Regular security audits and reviews will be conducted to identify potential vulnerabilities and enhance security measures as needed.