SHARECAL.IO

Security Program

ShareCal's Security

At ShareCal, we prioritize the security and privacy of our customers' data. As a leading enterprise scheduling platform, we take extensive measures to ensure that all information is protected. Our security framework adheres to industry standards such as SOC 2 Type 2 and ISO 27001, reinforced by Vanta, an automated platform ensuring continuous compliance. This document outlines ShareCal's comprehensive approach to security.

Table of Contents

---

1. Security Organization and Program

Security is an integral part of ShareCal's operations. We maintain an organized, comprehensive security program. ShareCal follows industry best practices aligned with ISO 27001 and SOC 2, including policies governing access control, cryptography, vulnerability management, and incident response.

Security Policies and Standards
Our policies cover data classification, secure server configuration, access management, vulnerability scanning, security monitoring, and incident management. These are continuously reviewed and updated to address emerging threats.

2. Personnel Security

We ensure that all personnel, including employees and contractors, follow strict security practices:

- **Background Checks**: All employees undergo background checks before hiring, ensuring they meet security criteria.
- **Security Awareness Training**: All new hires complete onboarding security training. Employees also participate in annual refresher courses to stay updated on security policies.

- **Onboarding and Offboarding**: User access is strictly managed through Role-Based Access Control (RBAC) and terminated within 24 hours of employee departure.

3. Product Security

ShareCal's scheduling solution incorporates several security features to protect users:

- **OAuth2 Integration**: ShareCal uses OAuth2 to securely access user data.
- **SAML SSO**: ShareCal supports SAML Single Sign-On, allowing enterprises to integrate with their existing identity providers for seamless and secure authentication.
- **Penetration Testing**: ShareCal undergoes regular security assessments, including third-party penetration testing.

Application Security
Our application development follows secure coding practices, aligned with OWASP Top 10 guidelines.

4. Infrastructure and Cloud Security

ShareCal operates a cloud-native infrastructure hosted on Azure. We employ a defense-in-depth strategy to ensure security at all layers:

- **Network Security**: ShareCal isolates sensitive workloads through network segmentation. Access is controlled via Azure Active Directory (AAD) and RBAC to restrict unauthorized access.
- **Encryption**: All data in transit is encrypted using TLS 1.2 or higher, while sensitive data at rest is encrypted using AES-256.
- **Identity & Access Management (IAM)**: Role-based access control enforces the principle of least privilege. Administrative access is secured with MFA.

5. Data Protection and Encryption

ShareCal follows strict data protection policies to safeguard user data:

- **Data Classification**: Data is classified based on its sensitivity to ensure it receives the appropriate level of protection.
- **Encryption in Transit and at Rest**: All sensitive data, including customer information, is encrypted at rest using AES-256 and in transit via TLS 1.2+.
- **Data Retention and Disposal**: Data is retained only as long as necessary to meet business and legal obligations. Data is securely erased following industry standards (NIST 800-88) when no longer needed.

6. Incident Response

ShareCal has a documented incident response plan to swiftly address any security incidents:

- **Monitoring and Alerts**: We continuously monitor our systems for suspicious activity using automated tools that trigger alerts for potential security events.
- **Incident Response Process**: In case of an incident, ShareCal follows a detailed process that includes identifying, containing, eradicating, and recovering from security incidents.
- **Tabletop Exercises**: We regularly conduct tabletop exercises to simulate incident scenarios, ensuring our team is well-prepared to respond effectively in real-world situations.

7. Business Continuity and Disaster Recovery

We have established robust business continuity and disaster recovery (BC/DR) policies to ensure service resilience:

- **Redundancy**: ShareCal leverages Azure's availability zones for redundancy and high availability.
- **Disaster Recovery**: We conduct annual disaster recovery tests, including full-scale data restoration, to ensure quick recovery in case of a system outage.
- **Backup Strategy**: Critical data is backed up daily and encrypted to prevent data loss.

8. Compliance

ShareCal complies with multiple industry standards and regulations to maintain the highest level of security:

- **SOC 2 Type 2**: We undergo regular SOC 2 Type 2 audits to validate our internal controls for data security and privacy.
- **GDPR Compliance**: We follow GDPR guidelines for data processing and handling, ensuring that customer privacy is protected.

Conclusion

At ShareCal, security is our top priority. We are committed to maintaining a secure platform through continuous improvement, regular audits, and adherence to best practices. Our goal is to provide users with a secure, reliable, and efficient scheduling experience.

For more information or to request our compliance documentation, contact us at security@sharecal.io.