SPOTICA SECURITY ATTESTATION

Introduction

This Security Attestation document provides an overview of the security controls, practices, and measures implemented by Spotica Ltd., the provider of the Spotica Platform Software as a Service (SaaS) application. This document is intended to give our customers and stakeholders insights into the security posture of our SaaS application.

Security Controls and Practices

1. Security Governance

1.1 **Information Security Policy.** Spotica Ltd. maintains a comprehensive Information Security Policy that outlines the principles and guidelines governing the protection of information assets, including those associated with the Spotica Platform. This policy is regularly reviewed and updated to address evolving security threats.

1.2 **Security Awareness and Training.** All employees and relevant stakeholders undergo regular security awareness training to ensure a strong security culture. Training includes topics such as data protection, secure coding practices, and response to security incidents.

2. Data Security

2.1 **Data Encryption.** Data transmitted between users and the Spotica Platform servers is encrypted using industry-standard protocols, such as TLS, to protect against eavesdropping and data interception.

2.2 **Data Storage Customer.** data is securely stored using encryption-at-rest mechanisms. Access controls and authentication mechanisms are in place to ensure that only authorized personnel can access sensitive data.

2.3 **Data Backups.** Regular data backups are performed to prevent data loss. Backup procedures include testing the restoration process to ensure data integrity.

3. Access Controls

3.1 **Authentication.** User authentication is enforced through strong password policies and includes multi-factor authentication (MFA) on all platforms and applications. Access to sensitive areas of the Spotica Platform is restricted based on the principle of least privilege.

3.2 **Authorization.** Role-based access controls (RBAC) are implemented to ensure that users have the necessary permissions to perform their tasks. Access rights are regularly reviewed and updated as needed.

4. Infrastructure Security

4.1 **Network Security.** Network security measures, including firewalls and web application firewalls, are in place to safeguard against unauthorized access and malicious activities.

4.2 **Hosting Environment.** The Spotica Platform is hosted in the secure and compliant AZURE data centre, which adheres to industry-recognized standards for physical and environmental security.

4.3 **Redundancy.** The Spotica Platform is hosted across more than one AZURE instance across the globe with the ability to failover to a different region if the need arise.

5. Incident Response

5.1 **Incident Monitoring and Response.** Spotica Ltd. maintains a robust incident response plan to detect, respond to, and mitigate security incidents promptly. Incident response procedures are regularly tested in simulated environments and updated to address emerging threats.

6. Compliance and Certifications

6.1 **Regulatory Compliance**. Spotica Ltd. is committed to complying with applicable data protection and privacy regulations (please refer to our Data Privacy Notice).

6.2 **Third-Party Security Assessments.** Periodic third-party security assessments and audits are conducted by our major banking and advisory clients (with integrated services into the platform) to validate the effectiveness of security controls and identify areas for improvement.

Conclusion

This Security Attestation affirms Spotica Ltd.'s commitment to the security and privacy of the Spotica Platform. We continuously strive to enhance our security posture and maintain transparency with our customers and stakeholders.

For any inquiries or additional information regarding the security measures outlined in this attestation, please contact support at support@spotica.io.