EVÖQ SECURITY POLICY

At EVÖQ, we prioritize the security and confidentiality of our users' data. This **Security Policy** outlines the measures we implement to protect the platform, personal data, transactions, and other sensitive information from unauthorized access, misuse, and potential breaches. By using the EVÖQ platform, you acknowledge and agree to the practices described in this policy.

1. Introduction

EVÖQ is committed to maintaining a secure environment for its users and protecting personal and business data. This Security Policy is designed to outline our approach to cybersecurity, data protection, and privacy, ensuring compliance with applicable laws, regulations, and industry standards.

Our platform handles a wide range of personal and sensitive data, including account credentials, transaction histories, and user-generated content. As such, we are committed to deploying advanced security technologies and maintaining stringent internal practices to safeguard this information.

2. Data Encryption and Transmission

We utilize strong encryption techniques to secure data both during transmission and while it is stored in our systems. This ensures that any sensitive data exchanged between the user's device and our servers remains confidential and protected from unauthorized access.

- **Encryption Protocols**: We use **Secure Socket Layer (SSL)**/ **Transport Layer Security (TLS)** protocols to encrypt data during transmission.
- **End-to-End Encryption**: All payment transactions processed on the platform are encrypted with end-to-end encryption to protect financial data and payment details.
- **Encryption of Stored Data**: Sensitive data, including user credentials, financial information, and other personal data, are stored in an encrypted format to prevent unauthorized access.

3. Access Control and Authentication

We apply strict access control policies to ensure that only authorized personnel have access to sensitive data. Access to personal data, platform management, and other confidential information is granted based on the principle of **least privilege**.

- **Multi-Factor Authentication (MFA)**: We require Multi-Factor Authentication (MFA) for platform administrators and users accessing sensitive account settings to provide an additional layer of protection.

- **User Authentication**: Users are required to create strong passwords and are encouraged to change them regularly. We also offer support for two-factor authentication (2FA) to ensure secure login.
- **Role-Based Access Control**: Access to platform features and user data is restricted based on the user's role, ensuring that only authorized personnel can access certain functions.

4. Secure Software Development Practices

Security is built into our platform from the ground up. We adopt a secure software development life cycle (SDLC) to ensure that security vulnerabilities are identified and mitigated throughout the development and maintenance phases.

- **Code Review and Testing**: All code is reviewed and tested for security vulnerabilities. We use automated testing tools to identify potential issues such as SQL injection, cross-site scripting (XSS), and other common attack vectors.
- **Third-Party Libraries and Dependencies**: We regularly review and update third-party libraries and dependencies to mitigate vulnerabilities arising from outdated or insecure software components.

5. Data Backup and Disaster Recovery

We ensure that regular data backups are performed to protect against data loss due to unforeseen events such as system failures, cyberattacks, or natural disasters. Our disaster recovery processes ensure rapid recovery of the platform in the event of a data breach, system crash, or any form of data corruption.

- **Automated Backups**: All critical data is backed up regularly in encrypted form and stored in a secure offsite location to prevent data loss.
- **Disaster Recovery Plan**: We maintain a robust disaster recovery plan, including predefined protocols for restoring data and platform functionality, and regularly test our recovery procedures to ensure quick restoration of services.
- **Data Retention and Backup**: Data is backed up on a periodic basis, and retention policies are in place to ensure that data is kept for the required period and disposed of securely when no longer needed.

6. Network and System Security

To protect the platform's infrastructure, we implement a wide range of network security measures designed to prevent unauthorized access, malware attacks, and other security threats.

- **Firewalls and Intrusion Detection**: We use firewalls and intrusion detection systems (IDS) to monitor and control network traffic, identifying and blocking any suspicious activity that could indicate a security breach.
- **Regular Security Audits**: We conduct regular security audits to identify potential vulnerabilities in our network infrastructure, system architecture, and web applications.
- **Anti-Malware and Anti-Virus Software**: All servers and devices accessing our network are protected by up-to-date anti-malware and anti-virus software to prevent malware infections.

7. User Data Privacy and Protection

We recognize that privacy is a fundamental aspect of security. We are committed to protecting the privacy of our users by implementing strict measures to ensure that personal data is handled in compliance with data protection laws such as the **General Data Protection Regulation (GDPR)**.

- **Data Minimization**: We only collect personal data that is necessary for the provision of services and ensure that it is securely stored.
- **Third-Party Data Processors**: We ensure that any third parties with access to user data are compliant with data protection laws and have appropriate security measures in place.
- **User Consent**: We obtain explicit user consent for data processing activities and provide users with options to manage their data preferences, including opting out of non-essential data processing.
- **User Rights**: Users have the right to request access to, rectification of, and deletion of their personal data, as well as to withdraw consent for data processing at any time.

8. Incident Response and Reporting

In the event of a security incident, EVÖQ follows a structured incident response process to mitigate the impact and protect user data.

- **Incident Detection and Monitoring**: We continuously monitor the platform for any suspicious activity, and we have automated systems in place to detect potential threats in real-time.
- **Incident Response Plan**: We have an incident response plan in place that includes protocols for identifying, responding to, and recovering from security breaches.

- **Data Breach Notifications**: In the event of a data breach, we will promptly notify affected users and regulatory bodies as required by law, providing details of the breach and steps taken to mitigate the risk.
- **Security Logs**: We maintain security logs of all incidents for audit purposes and use these logs to identify areas for improvement in our security practices.

9. Employee Training and Awareness

We recognize that employees are one of the most important elements of our security posture. As part of our commitment to security, all employees and contractors undergo regular security training to identify potential risks and adopt safe practices.

- **Security Awareness Training**: All employees receive mandatory security awareness training that covers topics such as phishing, password security, and data protection.
- **Access Control for Employees**: Employees are granted access to user data and systems based on their job roles and responsibilities. Their access is reviewed regularly to ensure it aligns with their duties.

10. Third-Party Security

We are committed to ensuring that any third-party service providers with access to our platform or user data follow stringent security measures.

- **Third-Party Audits**: We conduct security audits of our third-party providers to ensure they meet our security and privacy requirements.
- **Vendor Contracts**: We have contractual agreements in place with third-party vendors, specifying security and confidentiality obligations.

11. Compliance with Legal and Regulatory Requirements

EVÖQ complies with all relevant security and data protection regulations, including the **General Data Protection Regulation (GDPR)**, **Data Protection Act (DPA)**, and other applicable privacy laws.

- **Data Protection Officer (DPO)**: We have appointed a Data Protection Officer (DPO) to oversee compliance with data protection and security laws.
- **Regulatory Audits**: We cooperate with regulatory bodies to ensure ongoing compliance and undergo audits as required by law.

12. Review and Update of Security Practices

We continually assess and update our security practices to address new threats and vulnerabilities. This Security Policy is reviewed regularly and updated as necessary to reflect changes in laws, regulations, and emerging security threats.

---

13. Contact Information

If you have any questions or concerns about this Security Policy or if you would like more information regarding our security practices, please contact us at:

Email: [Support@evoqstudios.com]
Address: [86-90 Paul Street, London, EC2A 4NE]