Information Security Policy

1. Introduction

PsyConnect is committed to maintaining the confidentiality, integrity, and availability of the data we handle. This Information Security Policy establishes the guidelines and practices to protect our platform, data, and users from security threats, ensuring compliance with legal and industry standards.

2. Objectives

The primary objectives of this policy are:

- To safeguard the personal and sensitive data of PsyConnect users.
- To maintain the secure operation of the PsyConnect platform.
- To protect against unauthorized access, data breaches, and other security threats.
- To ensure compliance with applicable laws, including the GDPR.

3. Scope

This policy applies to all information systems, processes, and data managed by PsyConnect, as well as to Ruth and Francisco Flores, the sole administrators of the platform.

4. Roles and Responsibilities

- **Administrators (Ruth and Francisco Flores)**:
  - Manage and oversee all security practices.
  - Perform regular monitoring and maintenance of the PsyConnect platform.
  - Respond to security incidents promptly and effectively.
- **Third-Party Providers (e.g., Wix)**:
  - Ensure compliance with security requirements as outlined in service agreements.
  - Provide robust infrastructure and security measures as part of the hosting and operational framework.

5. Security Measures

PsyConnect employs a comprehensive set of security measures to protect data and ensure system resilience.

5.1. Access Control

- Access to data is restricted to Ruth and Francisco Flores, based on their roles as administrators.
- Role-based permissions provided by Wix ensure that therapists and clients can only access data relevant to their activities on the platform.
- Multi-factor authentication (MFA) is enabled for administrator access.

5.2. Data Encryption

- All sensitive data is encrypted in transit using HTTPS/SSL protocols and at rest using advanced encryption standards.
- Wix's infrastructure ensures end-to-end encryption for all hosted data.

5.3. User Authentication

- Users are required to create strong passwords, meeting defined complexity requirements.
- Two-factor authentication (2FA) is available for additional security.

5.4. Platform Security

- Wix provides security certifications, including ISO 27001 and PCI DSS, ensuring compliance with industry standards.
- Automated tools monitor for vulnerabilities, unauthorized access, and other threats 24/7.
- Regular updates and patches are applied to ensure platform integrity.

5.5. Physical Security

- Data hosting facilities are managed by Wix and include physical security measures such as surveillance, restricted access, and disaster recovery protocols.

5.6. Backup and Recovery

- Regular backups are performed to ensure data availability in case of an incident.
- Recovery protocols are in place to restore operations quickly after a disruption.

6. Incident Management

PsyConnect follows a structured approach to detect, respond to, and mitigate security incidents.

6.1. Incident Detection

- Wix's 24/7 monitoring tools detect anomalies and potential breaches in real time.
- Ruth and Francisco review alerts and investigate flagged activities.

6.2. Response Plan

1. Contain the incident to prevent further damage.
2. Analyse the root cause and identify affected data or systems.
3. Mitigate risks and restore secure operations.

6.3. Notification

- Affected users and relevant regulatory authorities will be notified of incidents involving personal data breaches within 72 hours, if required.

7. Security Audits and Assessments

- PsyConnect conducts periodic reviews of security measures to identify and address vulnerabilities.
- Wix's infrastructure undergoes regular third-party audits to maintain compliance with security standards.

8. Acceptable Use

All users of the PsyConnect platform must adhere to the following:

- Avoid sharing sensitive personal data outside secure communications on the platform.
- Maintain secure login credentials and avoid sharing them with others.
- Report any suspicious activity or security concerns immediately.

9. Compliance and Legal Requirements

- PsyConnect adheres to applicable legal and regulatory frameworks, including the GDPR.
- Third-party providers, such as Wix, are required to comply with these frameworks through service agreements.

10. Policy Maintenance

- Ruth and Francisco Flores review and update this policy annually or when significant changes occur in the operational or regulatory landscape.

11. Contact Information

For enquiries related to information security or to report a security incident, contact:

- **Email**: admin@psyconnect.co.uk
- **Phone**: 07735082994

Updated: 9 December 2024