MTHFRSUPPORT
Pioneers in Health. Science. Genetics.

Security Assessment Policy

1. Purpose

The purpose of this policy is to establish guidelines and procedures for conducting regular security assessments to identify vulnerabilities, evaluate risks, and ensure the ongoing security of our business. This policy outlines the framework for assessing the effectiveness of security controls and implementing necessary improvements to protect sensitive information and maintain regulatory compliance.

2. Scope

This policy applies to all aspects of the remote business, including systems, applications, networks, devices, and data, accessed and operated by employees.

3. Security Assessment Measures

3.1 Vulnerability Assessments

- Regular vulnerability assessments will be conducted on all systems, applications, and networks used by employees.
- Vulnerability scans will be performed using reputable scanning tools to identify potential weaknesses and security gaps.

3.2 Penetration Testing

- Periodic penetration tests will be conducted to simulate real-world attacks and assess the effectiveness of security controls.
- External and internal penetration tests will be performed to identify potential breaches from both outside and within the network.

3.3 Security Audits

- Independent security audits will be conducted by third-party experts to evaluate the overall security posture of the remote healthcare business.

- Audits will encompass technical, administrative, and physical security measures.

4. Assessment Planning and Execution

4.1 Assessment Frequency

- Vulnerability assessments will be conducted every 6 months.
- Penetration tests will be conducted annually.
- Security audits will be conducted biennially.

4.2 Test Environment and Scope

- Security assessments will be conducted in controlled environments that replicate working conditions.
- The scope of assessments will cover all systems, applications, networks, and devices used by employees.

5. Risk Management and Mitigation

5.1 Assessment Reporting

- Assessment results, including vulnerabilities identified, risk ratings, and recommended actions, will be documented in detailed reports.
- Reports will be shared with relevant stakeholders.

5.2 Risk Prioritisation

- Identified vulnerabilities and risks will be prioritised based on severity and potential impact on sensitive data and business operations.

5.3 Remediation and Action Plan

- An action plan will be developed to address and mitigate identified vulnerabilities and risks.
- Clear timelines and responsible parties will be assigned for implementing corrective measures.