Review Date- 01/10/2025

Trinity Support Services: Information Security Policy

1. Purpose

This Information Security Policy establishes a framework for managing and protecting sensitive information within Trinity Support Services, a provider of Edge of Care Services and Return Home Interviews. This policy aims to safeguard client data, ensure regulatory compliance, and maintain client and stakeholder trust.

2. Scope

This policy applies to all Trinity Support Services employees, contractors, and third parties who access, process, or manage company information or resources, including but not limited to Edge of Care Service data and Return Home Interview records.

3. Policy Objectives

To protect all confidential and sensitive data related to our clients, staff, and business processes from unauthorised access, modification, disclosure, or destruction.
To comply with all relevant legal, regulatory, and contractual requirements, including but not limited to the UK Data Protection Act 2018 and the General Data Protection Regulation (GDPR).
To ensure the reliability and integrity of data through clear security controls and procedures.

4. Responsibilities

Senior Management: Ensure policy compliance, allocate resources for information security, and promote an environment of data protection.
IT Department: Implement and maintain technical security measures, monitor systems, and respond to incidents.
Employees and Contractors: Adhere to this policy and report any suspected security breaches or vulnerabilities.

5. Data Classification

All data within Trinity Support Services is classified into three categories:

Confidential Data: Includes personal information related to clients, staff, and sensitive client service information such as Return Home Interview details. This data requires the highest level of protection.
Internal Data: Data necessary for business operations but not classified as confidential, which still requires restricted access.
Public Data: Information intended for public disclosure and does not require security controls.

6. Access Control

Access to Confidential Data is limited to authorised personnel based on job responsibilities.

All employees and contractors are required to use multi-factor authentication (MFA) when accessing confidential systems.

User accounts are deactivated immediately upon termination of employment or contract.

7. Data Protection

Encryption: Confidential Data must be encrypted both at rest and in transit. Approved encryption standards must be used.

Data Storage: Sensitive client data, including Edge of Care and Return Home Interview records, must be stored on secure servers with restricted access.

Data Retention: Client information will only be retained as long as necessary and in compliance with legal requirements. After the retention period, data must be securely deleted.

8. Network and System Security

Firewalls and Intrusion Detection: All systems must be protected by firewalls and monitored for suspicious activity.

Regular Updates: Software, including antivirus programs, operating systems, and applications, must be kept up-to-date with security patches.

Access Monitoring: User activity and access logs must be reviewed regularly to detect unauthorised access attempts.

9. Incident Response

Incident Reporting: Employees are required to report suspected or confirmed security incidents to the IT department immediately.

Incident Response Team (IRT): An Incident Response Team will be activated to manage and mitigate any information security incidents, ensuring minimal impact on operations.

Root Cause Analysis: After any incident, a thorough investigation will be conducted to identify the cause and prevent recurrence.

10. Training and Awareness

All employees and contractors must complete mandatory information security and data protection training at the start of employment and annually thereafter. The training will cover best practices in handling confidential data, phishing awareness, and reporting procedures for suspected security incidents.

11. Physical Security

Office Access Control: Access to areas where sensitive data is stored, processed, or managed must be restricted to authorised personnel.

Device Management: All company-owned devices must be locked when unattended and encrypted to prevent unauthorised access.

12. Third-Party Security

Third parties who handle Trinity Support Services’ data must comply with this Information Security Policy or equivalent standards. Vendors must sign confidentiality agreements and undergo periodic security assessments.

13. Compliance and Review

Audits: Regular audits will be conducted to assess compliance with this policy.

Policy Review: This policy will be reviewed and updated annually or as needed to comply with regulatory or organisational changes.

14. Disciplinary Actions

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

15. Approval and Acceptance

This policy is approved by Trinity Support Services' management and is effective as of the date below. All employees, contractors, and relevant third parties are required to read, understand, and adhere to this policy.

Contact Information

For questions or concerns regarding this policy, please contact the Company Directors:

Zoe Ashman- zoe.ashman@trinitysupportservices.info

Tracy Dean- Tracy.dean@trinitysupportservices.info