Training Needs Analysis (TNA) & Communication Plan

Approved By: Dr Serena Haywood (SIRO) | **Last Reviewed:** 29/12/2025

1. Audience Analysis & Training Requirements

We have analyzed the roles within CheckTick to ensure training is proportionate to the risk associated with each role.

Staff Group	Core Requirement	Specialized Requirement	Frequency
All Staff / Founders	NHS Data Security Awareness (L1)	GDPR & Caldicott Principles	Annual
Technical Staff (CTO)	NHS Data Security Awareness (L1)	OWASP Top 10, Vault Management, Secure SDLC	Annual + Ongoing
DPO / SIRO	NHS Data Security Awareness (L1)	DPIA Methodology, Incident Management, Risk Register	Annual + Ongoing
Future Support Staff	NHS Data Security Awareness (L1)	Verifying Identities, Handling SARs, Data Minimization	At Induction

2. Delivery Methods

- **Formal Learning:** Completion of the NHS Digital Data Security Awareness modules (e-Learning).
- **Technical Workshops:** Internal "Security-by-Design" walkthroughs for infrastructure changes.
- **Briefings:** Security updates during monthly Founders' Meetings (documented in Board Minutes).
- **Self-Directed:** Ongoing review of the Security Overview.

3. Communication & Awareness Strategy

Information is made available to staff through the following channels:

- **The 'Master Index':** Centralized compliance repo for all policies.
- **UI Documentation Portal:** Public-facing docs for transparency on system security.
- **Slack Integration:** Automated alerts for Dependabot (vulnerabilities) and GitHub security events.
- **Policy Briefings:** All new or updated policies are discussed and signed off at the board level.

4. Evaluation of Effectiveness

We measure the impact of our TNA through:

1. **Compliance Spot-Checks:** Testing staff knowledge on the Incident Response Plan.
2. **Audit Logs:** Monitoring if staff are following secure access protocols (e.g., using MFA).
3. **Training Log:** Maintaining 100% completion status in `compliance/training.md`.