Security-awareness training policy

SAMPLE · FICTIONAL COMPANY

Meridian Dental Group — Sample Company · Adopted October 5, 2026 (illustrative) · Filled from the pack's plain-English template in about ten minutes; the questionnaire sentence about having a training program is now true in writing.

1. Purpose

Meridian Dental Group trains every member of staff to recognize and respond to common security threats — phishing, social engineering, payment fraud, and AI-era scams — so that patient, financial, and business information stays protected.

2. Who this covers

All employees and long-term contractors, full-time and part-time, in every role: clinical, front desk, billing, and administration. New hires complete the training within 30 days of their start date.

3. The training program

- Short video modules (3–5 minutes each) covering phishing & email scams, passwords & MFA, social engineering, data handling & privacy, remote work security, incident reporting, and AI-era scams & deepfakes.
- Each module ends with a short quiz; a passing quiz creates a dated completion record for that employee.
- Every employee completes all assigned modules at least once every 12 months.

4. How completion is tracked

The office manager maintains the completion log and files each completion record in the evidence pack behind the evidence register. The log is reviewed for gaps at the end of each rollout window and before each insurance renewal.

5. Reporting security concerns

Anyone who suspects a scam, clicks a suspicious link, or receives an unusual payment request reports it to the office manager immediately. Reporting is always the right move: no employee will ever be penalized for reporting a concern or for taking two minutes to verify an unusual request before acting.

6. Review

This policy is reviewed annually — next review October 2027 — and whenever the practice's tools or team change materially.

Priya Nair
Dr. Priya Nair, Managing Partner — adopted October 5, 2026 (illustrative)

Dana Reyes
Dana Reyes, Office Manager — policy administrator