

DRAFT · NOT IN EFFECT UNTIL APPROVED

Information Security Policy

Sample Dental Group · Policy

Document control	
Document owner	Practice Administrator
Approved by	Managing Partner Signature: _____ Date: _____
Version	0.1 (starter draft, October 16, 2026)
Review cycle	At least annually, and after a significant incident or change
Classification	Internal

Purpose

This policy sets out how Sample Dental Group protects its information, systems and operations, and who is accountable for doing so.

Scope

This document applies to all Sample Dental Group staff, contractors and service providers, including the outsourced IT provider, and to every system that stores, processes or carries patient or practice information.

Policy statements

1. Sample Dental Group manages cybersecurity risk as a business risk. Leadership sets the direction, provides resources, and reviews results.
2. One named role, the [Security Lead], is accountable for planning, resourcing and carrying out the security program.
3. Everyone who uses Sample Dental Group's systems must follow this policy and the standards and procedures that support it.
4. Security requirements in laws, regulations and customer contracts that apply to Sample Dental Group are identified, recorded and met.
5. Access to systems and information is granted only as needed for a person's role and is removed when no longer needed.
6. Security incidents and suspected incidents must be reported immediately to [the Security Lead or IT help desk].
7. Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

Supporting documents

8. This policy is supported by the standards, procedures and plans listed in the documentation plan, including access control, authentication, incident response, backup and vendor management.
9. Where a supporting document conflicts with this policy, this policy applies until the conflict is resolved by the [Security Lead].

Communication

10. This policy is given to all staff and contractors when they join and whenever it changes.
11. Staff acknowledge the policy in writing or electronically at least once a year.

Exceptions

Exceptions to this document must be requested in writing, approved by the Practice Administrator, and recorded in the exception log with a compensating control and an expiry date.

Review

The document owner reviews this document at least annually, and after a significant incident or change. Changes are approved by the Managing Partner and recorded below.

Revision history

Version	Date	Change	Approved by
0.1	October 16, 2026	Starter draft generated from the NIST CSF 2.0 assessment	

Framework mapping

Once adopted and followed, this document supports the following NIST CSF 2.0 requirements.

Subcategory	Requirement
GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced
GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission
GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed
GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced

Text in [brackets] must be replaced with Sample Dental Group's own details before this document is used. This is a starting point prepared from the assessment results; it does not describe current practice until it has been tailored, approved and put into effect.