

CYBER SECURITY CONTROLS SUMMARY

Sample Dental Group (made up) · Renewal or application Dec 1, 2026 · Prepared Oct 16, 2026

14 employees · Sensitive data: Patient health records for about 6,800 patients; card payments go through the processor's terminal · Current insurer: Sample Mutual Insurance (made up) · Broker: Example Insurance Brokers (made up)

Control	Status	Coverage	Evidence on file (date, source)
Is multi-factor authentication (MFA) required for all email access, including webmail and phones?	Yes	14 of 14 mailboxes with MFA enforced	E-01 MFA or conditional-access report from the email admin console (Oct 14, 2026, IT provider or MSP); E-02 User list showing MFA registered for every mailbox (Oct 14, 2026, IT provider or MSP)
Is MFA required for all remote access to the network (VPN, remote desktop, remote management tools)?	Partly	1 of 2 remote-access paths behind MFA	E-03 VPN or remote-access settings showing MFA required (Oct 6, 2026, IT provider or MSP)
Is MFA required for all administrator and privileged accounts, including cloud, backup and email admin?	Yes	4 of 4 admin accounts with MFA	E-05 Admin account list with MFA status, including IT provider and break-glass accounts (Oct 6, 2026, IT provider or MSP)
Is remote desktop (RDP) or any other remote-access service closed to the open internet?	Partly		E-06 External scan showing no remote desktop or admin ports open (Oct 2, 2026, Our review); E-07 Firewall rule review (Oct 2, 2026, Our review)
Do staff use separate accounts for administrator work, with everyday accounts lacking admin rights?	Yes		E-08 List of admin accounts and who holds them (Oct 6, 2026, IT provider or MSP)
Is access removed promptly when someone leaves the business?	Yes		E-09 Leaver checklist and one recent completed example (Sep 15, 2026, Client)
Is endpoint detection and response (EDR) or next-generation antivirus installed on every computer and server?	Yes	22 of 22 computers and servers with EDR	E-10 EDR console export listing every protected device (Oct 2, 2026, IT provider or MSP); E-11 RMM or asset list to compare it against (Oct 2, 2026, IT provider or MSP)
Are critical security updates applied within 30 days, or sooner when actively exploited?	Yes		E-12 RMM or update-tool patch compliance report (Oct 5, 2026, IT provider or MSP)
Are all operating systems and key software still supported by the vendor?	Yes, not proven		
Are systems scanned for vulnerabilities at least once a year?	No		
Are critical data and systems backed up at least weekly?	Yes	3 of 3 critical systems backed up	E-17 Backup job report listing systems, frequency and success (Sep 30, 2026, IT provider or MSP)
Is at least one backup copy offline, immutable or otherwise separated so ransomware cannot reach it?	Yes		E-18 Backup settings showing an offline or immutable copy with separate credentials (Sep 30, 2026, IT provider or MSP)
Has a restore from backup been tested successfully in the last 12 months?	Yes		E-19 Dated restore test record: what was restored and how long it took (Oct 7, 2026, Our review)

Control	Status	Coverage	Evidence on file (date, source)
Is incoming email filtered for malicious links and attachments, with SPF, DKIM and DMARC set up for the domain?	Partly		E-20 Email filtering settings (Oct 6, 2026, IT provider or MSP); E-21 SPF, DKIM and DMARC records, or a DMARC report (Oct 2, 2026, Our review)
Do all staff complete security awareness training at least once a year?	Yes		E-22 Training completion report with dates (Sep 10, 2026, Client)
Are phishing simulations run with staff?	Yes		E-23 Phishing test results with dates (Sep 18, 2026, Client)
Must payment and bank-detail change requests be verified by phone using a known number before money is sent?	Partly		
Does the business have a written incident response plan?	Partly		
Has the incident response plan been tested, for example with a tabletop exercise, in the last 12 months?	No		
Are security logs collected and monitored, by staff, the IT provider or a managed detection service?	No		
Is there an up-to-date list of the business's computers, servers and cloud services?	Yes, evidence out of date		E-29 Asset inventory with last-updated date (Nov 20, 2025, IT provider or MSP)
Are vendors with access to systems or sensitive data reviewed for security?	Partly		E-30 Vendor list with review dates (Sep 24, 2026, Client)
Are laptops and sensitive data encrypted?	Yes	6 of 6 laptops encrypted	E-31 Device encryption report (BitLocker or FileVault) (Oct 1, 2026, IT provider or MSP)
Are written security policies in place and approved by management?	Yes		E-32 Approved policies with approval dates (Sep 24, 2026, Client)

EXTERNAL CHECKS

Check	Result	Date
X-01 Email domain records (sampledental.example.com)	SPF v=spf1 include:spf.protection.outlook.com -all; DMARC v=DMARC1; p=none; rua=mailto:dmarc@sampledental.example.com	Oct 2, 2026
X-02 Remote desktop or admin ports open to the internet	Found: Firewall admin page on 203.0.113.18 (port 8443); no remote desktop	Oct 2, 2026
X-03 Expired or invalid certificates on public websites or VPN	None found	Oct 2, 2026
X-04 Staff accounts on the client's domain found in known breaches	Found: 3 staff addresses in older public breaches; passwords since changed	Oct 2, 2026

IMPROVEMENTS UNDER WAY

Control	Planned action	Target date
Is MFA required for all remote access to the network (VPN, remote desktop, remote management tools)?	Put every remote path behind MFA; remove remote tools nobody needs, including the IT provider's spares.	Nov 6, 2026

Control	Planned action	Target date
Is remote desktop (RDP) or any other remote-access service closed to the open internet?	Close inbound RDP and admin ports at the firewall; reach them only through a VPN with MFA.	Oct 31, 2026
Must payment and bank-detail change requests be verified by phone using a known number before money is sent?	Write a call-back rule for any new payee or changed bank details, using a number already on file, and train finance staff on it.	Oct 31, 2026
Are systems scanned for vulnerabilities at least once a year?	Run an internal and external scan and fix findings in priority order; repeat at least yearly.	Nov 20, 2026
Are security logs collected and monitored, by staff, the IT provider or a managed detection service?	Send security logs to a monitored service and keep them at least 90 days.	Feb 26, 2027
Is incoming email filtered for malicious links and attachments, with SPF, DKIM and DMARC set up for the domain?	Turn on advanced filtering and publish SPF, DKIM and a DMARC policy, moving to quarantine or reject.	Nov 30, 2026
Does the business have a written incident response plan?	Write a short plan: who to call, how to isolate systems, the insurer's hotline, and who may speak publicly.	Nov 13, 2026
Are all operating systems and key software still supported by the vendor?	Collect: Asset list with operating-system versions.	Oct 30, 2026
Has the incident response plan been tested, for example with a tabletop exercise, in the last 12 months?	Run a 90-minute tabletop exercise and fix what it shows.	Nov 20, 2026
Are vendors with access to systems or sensitive data reviewed for security?	List vendors with access, review the important ones yearly, and add security terms to contracts.	Nov 30, 2026
Is there an up-to-date list of the business's computers, servers and cloud services?	Collect again (older than 90 days): Asset inventory with last-updated date.	Nov 6, 2026

Prior incidents or claims (last three to five years): Yes. Email fraud on Oct 13, 2026: one \$18,400 vendor payment diverted; reported to the insurer and IC3 the same day; recall in progress.

These answers were reviewed with and confirmed by Dr. R. Example, managing dentist on Oct 15, 2026.

Evidence references (E-, X-) point to the Evidence Schedule addendum that follows.

Prepared by Alex Sample, CISSP, Example Security Partners, from interviews and the evidence listed. A status of Yes means answered Yes, with evidence collected within 90 days; each piece of evidence shows the control on the date given. It is not an audit opinion and does not replace the insurer's application.

ADDENDUM

EVIDENCE SCHEDULE

This is an index of the evidence behind the summary. The evidence itself is held by Sample Dental Group (made up) and is not attached, because exports and screenshots of security systems contain sensitive details. Any item can be provided on request by its reference, with sensitive details removed.

Ref	Control	Evidence	Dated	Held by	Status
E-01	Is multi-factor authentication (MFA) required for all email access, including webmail and phones?	MFA or conditional-access report from the email admin console	Oct 14, 2026	IT provider or MSP	Current
E-02	Is multi-factor authentication (MFA) required for all email access, including webmail and phones?	User list showing MFA registered for every mailbox	Oct 14, 2026	IT provider or MSP	Current
E-03	Is MFA required for all remote access to the network (VPN, remote desktop, remote management tools)?	VPN or remote-access settings showing MFA required	Oct 6, 2026	IT provider or MSP	Current
E-05	Is MFA required for all administrator and privileged accounts, including cloud, backup and email admin?	Admin account list with MFA status, including IT provider and break-glass accounts	Oct 6, 2026	IT provider or MSP	Current
E-06	Is remote desktop (RDP) or any other remote-access service closed to the open internet?	External scan showing no remote desktop or admin ports open	Oct 2, 2026	Our review	Current
E-07	Is remote desktop (RDP) or any other remote-access service closed to the open internet?	Firewall rule review	Oct 2, 2026	Our review	Current
E-08	Do staff use separate accounts for administrator work, with everyday accounts lacking admin rights?	List of admin accounts and who holds them	Oct 6, 2026	IT provider or MSP	Current
E-09	Is access removed promptly when someone leaves the business?	Leaver checklist and one recent completed example	Sep 15, 2026	Client	Current
E-10	Is endpoint detection and response (EDR) or next-generation antivirus installed on every computer and server?	EDR console export listing every protected device	Oct 2, 2026	IT provider or MSP	Current
E-11	Is endpoint detection and response (EDR) or next-generation antivirus installed on every computer and server?	RMM or asset list to compare it against	Oct 2, 2026	IT provider or MSP	Current
E-12	Are critical security updates applied within 30 days, or sooner when actively exploited?	RMM or update-tool patch compliance report	Oct 5, 2026	IT provider or MSP	Current

Ref	Control	Evidence	Dated	Held by	Status
E-17	Are critical data and systems backed up at least weekly?	Backup job report listing systems, frequency and success	Sep 30, 2026	IT provider or MSP	Current
E-18	Is at least one backup copy offline, immutable or otherwise separated so ransomware cannot reach it?	Backup settings showing an offline or immutable copy with separate credentials	Sep 30, 2026	IT provider or MSP	Current
E-19	Has a restore from backup been tested successfully in the last 12 months?	Dated restore test record: what was restored and how long it took	Oct 7, 2026	Our review	Current
E-20	Is incoming email filtered for malicious links and attachments, with SPF, DKIM and DMARC set up for the domain?	Email filtering settings	Oct 6, 2026	IT provider or MSP	Current
E-21	Is incoming email filtered for malicious links and attachments, with SPF, DKIM and DMARC set up for the domain?	SPF, DKIM and DMARC records, or a DMARC report	Oct 2, 2026	Our review	Current
E-22	Do all staff complete security awareness training at least once a year?	Training completion report with dates	Sep 10, 2026	Client	Current
E-23	Are phishing simulations run with staff?	Phishing test results with dates	Sep 18, 2026	Client	Current
E-29	Is there an up-to-date list of the business's computers, servers and cloud services?	Asset inventory with last-updated date	Nov 20, 2025	IT provider or MSP	Older than 90 days
E-30	Are vendors with access to systems or sensitive data reviewed for security?	Vendor list with review dates	Sep 24, 2026	Client	Current
E-31	Are laptops and sensitive data encrypted?	Device encryption report (BitLocker or FileVault)	Oct 1, 2026	IT provider or MSP	Current
E-32	Are written security policies in place and approved by management?	Approved policies with approval dates	Sep 24, 2026	Client	Current

EXTERNAL CHECKS ON FILE

Check	Result	Date
X-01 Email domain records (sampledental.example.com)	SPF v=spf1 include:spf.protection.outlook.com -all; DMARC v=DMARC1; p=none; rua=mailto:dmarc@sampledental.example.com	Oct 2, 2026
X-02 Remote desktop or admin ports open to the internet	Found: Firewall admin page on 203.0.113.18 (port 8443); no remote desktop	Oct 2, 2026
X-03 Expired or invalid certificates on public websites or VPN	None found	Oct 2, 2026
X-04 Staff accounts on the client's domain found in known breaches	Found: 3 staff addresses in older public breaches; passwords since changed	Oct 2, 2026

Only evidence that has been collected is listed; items requested but not yet received are not. Each item shows the control on the date given. Items older than 90 days are marked and will be refreshed before renewal.