CYBER INSURANCE PREP · APPLICATION READINESS REPORT

Riverbend Family Dental (sample)

Domain checked: glowewebsites.com
Prepared November 28, 2026 by Glowe Websites
Application / renewal due: 2027-01-15
23 of 23 checklist questions answered

37
READINESS / 100

Fix these before you apply

The questions many cyber applications treat as must-haves

Must-have	Today
Turn on MFA for all email	Partly
MFA on every remote-access path	No
MFA + separate admin accounts	No
Written call-back rule for bank changes	Not sure
One offline / immutable backup copy	No
EDR on every computer and server	Partly
Replace unsupported software and gear	Yes

Top fixes, in order

1. **One offline / immutable backup copy** · IT person or IT company · half a day **MUST-HAVE**
2. **MFA on every remote-access path** · Your IT person or IT company · 2-4 hours **MUST-HAVE**
3. **Written call-back rule for bank changes** · Owner + whoever pays bills · 30 minutes **MUST-HAVE**
4. **MFA + separate admin accounts** · Owner + IT person · 2-3 hours **MUST-HAVE**
5. **Turn on MFA for all email** · Whoever manages your email (you, your IT person or IT company) · 1-2 hours **MUST-HAVE**
6. **EDR on every computer and server** · IT person or IT company · half a day **MUST-HAVE**

Outside check of glowewebsites.com: grade **B** (87/100), details on page 'What anyone can see from outside'.

Your fix plan

Worst gaps first. Hand this page to whoever looks after your IT. When an item is done, the honest answer on the application becomes Yes. Items marked 'find out first' are questions you weren't sure about: check them before you answer.

1. One offline / immutable backup copy · MUST-HAVE · today: No

Fix: Keep one copy the main network can't change: an immutable/locked cloud backup, a backup service with a separate login + MFA, or a drive that is unplugged after each backup and stored away. Turn on backup encryption.
Who: IT person or IT company · Time: half a day · CIS IG1: 11.3, 11.4

2. MFA on every remote-access path · MUST-HAVE · today: No

Fix: Turn on MFA in each remote tool (most VPNs and remote-access apps have it built in). Remove remote tools nobody uses. Never leave remote desktop (RDP) open straight to the internet: put it behind a VPN or a gateway with MFA.
Who: Your IT person or IT company · Time: 2-4 hours · CIS IG1: 6.4

3. Written call-back rule for bank changes · MUST-HAVE · find out first · today: Not sure

How to check: Ask whoever pays the bills: what did you do the last time a vendor said 'our bank details changed'? Is it written down?
Fix: Write a one-line rule and give it to everyone who pays bills: 'Any new or changed bank details = we call the person back at the number already on file, and a second person signs off.' Keep a short log of each call-back (date, who, number called). Applications often ask whether this is written.
Who: Owner + whoever pays bills · Time: 30 minutes · CIS IG1: 14.2

4. MFA + separate admin accounts · MUST-HAVE · today: No

Fix: Turn on MFA on every admin login (registrar and DNS first: whoever controls them controls your email). Give admins a separate admin account they only use for admin work; daily email and browsing from a normal account.
Who: Owner + IT person · Time: 2-3 hours · CIS IG1: 6.5, 5.4

5. Turn on MFA for all email · MUST-HAVE · today: Partly

Fix: Turn on MFA for EVERY mailbox, including the owner, admin and shared logins people sign in to. Microsoft 365: turn on Security defaults (or a Conditional Access policy requiring MFA for all users). Google Workspace: enforce 2-Step Verification. Prefer an authenticator app or passkey over text-message codes.
Who: Whoever manages your email (you, your IT person or IT company) · Time: 1-2 hours · CIS IG1: 6.3

6. EDR on every computer and server · MUST-HAVE · today: Partly

Fix: Put an EDR tool on every computer and server, with updates automatic and alerts going to someone who watches them (your IT company, or a managed service). Microsoft 365 Business Premium already includes Defender for Business. Turn off autorun for USB drives. (EDR goes past CIS IG1's 'anti-malware' safeguard; insurers ask by name.)
Who: IT person or IT company · Time: half a day · CIS IG1: 10.1, 10.2, 10.3

7. Firewall on, RDP closed to the internet · find out first · today: Not sure

How to check: Ask your IT person which ports are open on the office router. Check Windows Security > Firewall on each PC. (We don't scan ports without the owner's signed permission: see the permission form.)
Fix: Close every port the business doesn't need on the router; put remote access behind a VPN with MFA. Turn the built-in firewall on on every computer. Write a one-page standard for how a new computer is set up.
Who: IT person or IT company · Time: 2-3 hours · CIS IG1: 4.1, 4.2, 4.4, 4.5, 4.6

8. Test a restore · today: No

Fix: Do a test restore now: a folder of files, the accounting file and one whole computer. Time it and write down the date and result. Repeat every 6 months. (Test restores are CIS safeguard 11.5, one step past IG1, but applications often ask.)
Who: IT person or IT company · Time: 2-4 hours · CIS IG1: 11.1

9. Yearly scam + phishing training · today: No

Fix: Run a 20-30 minute training once a year (and for every new hire): fake emails and texts, payment scams, passwords and MFA, public Wi-Fi, handling customer data, how to report a mistake fast. Many email-security and IT companies include practice phishing emails. Keep the attendance list: applications ask.
Who: Owner or IT company · Time: 1 hour a year · CIS IG1: 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8

10. Remove admin rights from daily accounts · today: No

Fix: Remove admin rights from daily accounts; keep one separate admin login per computer (or managed by the IT company). Change default passwords on routers, printers and cameras.
Who: IT person or IT company · Time: 1-2 hours · CIS IG1: 5.4, 4.7

11. One-page incident plan · today: No

Fix: Write a one-page incident plan: who is in charge, the phone numbers (insurer's claims hotline, bank fraud line, IT company, your agent), how staff report a problem, where backups are, and 'don't pay or delete anything before you call the insurer'. Print it and keep a copy off the network.

Who: Owner · Time: 1 hour · CIS IG1: 17.1, 17.2, 17.3

12. Joiner / leaver checklist · today: Partly

Fix: Make a one-page joiner/leaver checklist (every account a person can have). Turn off former staff accounts now, and review the account list every quarter.

Who: Owner / office manager · Time: 1 hour · CIS IG1: 6.1, 6.2, 5.3

13. Email filtering + SPF/DKIM/DMARC · today: Yes

Outside check: DMARC is set to monitor only (p=none): fake email from @glowewebsites.com is reported but not blocked.

Fix: Turn on the provider's advanced filtering (Microsoft Defender for Office 365 / Google's advanced protection settings). Publish SPF, turn on DKIM signing, and add DMARC (start at p=none with reports, move to p=quarantine). Add DNS filtering (often part of the EDR or firewall, or a filtering DNS service).

Who: Email admin / IT company · Time: 2-3 hours · CIS IG1: 9.2

14. Encrypt laptops, auto-lock screens · today: Partly

Fix: Turn on BitLocker (Windows) or FileVault (Mac) on every laptop and save the recovery keys somewhere safe. Set screens to lock after 5-15 minutes. Require a passcode on phones with work email.

Who: IT person or IT company · Time: 1 hour · CIS IG1: 3.6, 4.3

15. Turn on and keep audit logs · find out first · today: Not sure

How to check: Microsoft 365: Microsoft Purview > Audit (check it is on). Google Workspace: Admin console > Reporting > Audit and investigation.

Fix: Make sure audit logging is on in your email/cloud admin center and on servers and the firewall, and kept 90 days or more. Logs are what an incident team needs first.

Who: IT person or IT company · Time: 1 hour · CIS IG1: 8.1, 8.2, 8.3

16. Device, software and account list · today: No

Fix: Keep a one-sheet list (the spreadsheet in this report has a tab for it): device, user, operating system, security app, last update; software and who approved it; every user account. Review it every quarter.

Who: Owner / office manager · Time: 1-2 hours · CIS IG1: 1.1, 1.2, 2.1, 2.3, 5.1

17. Password manager for the team · today: Partly

Fix: Give everyone a business password manager (1Password, Bitwarden, Keeper, or the one in your browser for very small teams). Move shared logins into a shared vault, change reused passwords, and use MFA wherever offered.

Who: Owner + team · Time: 2 hours · CIS IG1: 5.2, 4.7

18. Map and trim sensitive data · today: Partly

Fix: Write down what sensitive data you keep, where, and for how long. Limit those folders to the people who need them. Delete or shred what you don't need; wipe old computers and drives before they leave. Let the card processor hold card numbers instead of keeping them yourself.

Who: Owner / office manager · Time: 2-3 hours · CIS IG1: 3.1, 3.2, 3.3, 3.4, 3.5

How you'd honestly answer the application today

Each line is the way cyber applications commonly word the question, and your answer from the checklist. Carriers word them differently; the substance is the same.

Application question	Today	Your note / what we saw
Do you require multi-factor authentication (MFA) for all remote access to email (including webmail and cloud email)?	Partly	
Do you require MFA for all remote network access (VPN, remote desktop (RDP), remote-access tools)?	No	
Is MFA required for all privileged / administrator accounts? Are admin accounts separate from day-to-day accounts?	No	
Do you use MFA for online banking and payment systems? Do funds transfers above a set amount need dual authorization?	Yes	
Do you verify all requests to transfer funds or change vendor/supplier/customer bank details by an out-of-band method (for example a call-back to a known number) before acting?	Not sure	
How often do you back up critical data and systems? Are backups automated?	Yes	
Are backups kept offline, segregated from your network, or immutable? Are backups encrypted and protected by separate credentials/MFA?	No	
Have you tested restoring from backups in the last 6 / 12 months? How long would a full restore take?	No	
Do you use an endpoint detection and response (EDR) tool on all endpoints and servers? Which vendor? Is it monitored (24/7 or by an MSP)?	Partly	Office PC only, not the front-desk laptops
Do you have a patch management process? How quickly are critical and high-severity patches applied?	Yes	
Do you use any end-of-life or unsupported software or hardware? If so, how is it isolated?	Yes	
Do you have a firewall? Is RDP (or SMB, or remote access) exposed to the internet?	Not sure	
Do end users have local administrator rights on their computers?	No	
Do you have a password policy? Do employees use a password manager?	Partly	
Do you have a process to grant and revoke access promptly when employees join, change roles or leave?	Partly	
Do you provide security awareness training to employees at least annually? Do you run phishing simulations?	No	
Do you use advanced email filtering/sandboxing? Have you implemented SPF, DKIM and DMARC? Do you use web/DNS filtering?	Yes	Outside check: DMARC is set to monitor only (p=none): fake email from @glowewebsites.com is reported but not blocked.
Is sensitive data encrypted on laptops and mobile devices? Do devices lock automatically?	Partly	
What types of sensitive records do you hold and roughly how many? Is access restricted? Do you accept card payments and are you PCI compliant?	Partly	

Application question	Today	Your note / what we saw
Do you collect and retain security logs? For how long?	Not sure	
Do you maintain an inventory of hardware, software and user accounts?	No	
Do third-party vendors have remote access to your systems? Is it MFA-protected and monitored? Do you have an inventory of service providers?	Yes	
Do you have a written incident response plan? Has it been tested?	No	

Facts the application will ask for

What the business does: Dental office
People with a work email or computer: 6-15
Work email runs on: Microsoft 365
Who looks after your IT: An IT company (MSP)
Roughly how many people's sensitive records you hold: 1,000-10,000
You take card payments: Yes, through a card processor/terminal only

What anyone can see from outside

glowewebsites.com · grade B (87/100) · checked 2026-11-28. Public information only: DNS records, the public homepage loaded once, certificate logs, spam blocklists, the registry record.

- **DMARC is set to monitor only (p=none): fake email from @glowewebsites.com is reported but not blocked.**
  Fix: After checking the reports, change the DMARC policy to p=quarantine, then p=reject.
- **No anti-framing header: other sites can show this page inside a frame (clickjacking).**
  Fix: Add X-Frame-Options: SAMEORIGIN (or CSP frame-ancestors 'self').
- **Public certificate logs (crt.sh) didn't answer in time.**
- **SPF lists which servers may send this domain's email.**
- **HTTPS works with a trusted certificate (issuer unknown).**
- **No outdated software visible in the page source.**
- **Domain registered until 2027-09-14 (NameCheap, Inc.).**
- **The web and mail servers we found (2) are on none of the spam blocklists we asked.**

Want deeper tests (open ports, remote desktop exposure, a web vulnerability scan)? Those need the owner's signed permission first: scorecard.glowewebsites.com/permission. Nothing deeper runs without it.

CIS Controls v8.1, Implementation Group 1 (essential cyber hygiene)

From your answers: **10 of 56** IG1 safeguards in place, 18 partly. IG1 is the published starting set for small businesses; many application questions map to it.

- ✗ **1.1** Keep a detailed list of company devices
- ✗ **1.2** Deal with unknown devices on the network
- ✗ **2.1** Keep a list of the software you use
- ✓ **2.2** Use only software its maker still supports
- ✗ **2.3** Remove software nobody approved
- ½ **3.1** Have a process for handling data
- ½ **3.2** Know what sensitive data you hold and where
- ½ **3.3** Limit who can open which files
- ½ **3.4** Keep data only as long as needed
- ½ **3.5** Dispose of data and old devices securely
- ½ **3.6** Encrypt laptops and phones
- ✗ **4.1** Set up computers securely (a written standard)
- ✗ **4.2** Set up routers and firewalls securely
- ½ **4.3** Lock screens automatically
- ✗ **4.4** Firewall on servers
- ✗ **4.5** Firewall on every computer
- ✗ **4.6** Manage devices and software securely (no old remote-access protocols)
- ½ **4.7** Change default passwords and accounts
- ✗ **5.1** Keep a list of user accounts
- ½ **5.2** Unique passwords
- ½ **5.3** Turn off accounts nobody uses
- ✗ **5.4** Admin rights only in separate admin accounts
- ½ **6.1** A process for giving access
- ½ **6.2** A process for removing access
- ½ **6.3** MFA on internet-facing apps (email, banking, cloud)
- ½ **6.4** MFA on remote access
- ✗ **6.5** MFA on admin access
- ✓ **7.1** A process for finding weaknesses (patching plan)
- ✓ **7.2** A process for fixing them
- ✓ **7.3** Automatic operating-system updates
- ✓ **7.4** Automatic app updates
- ✗ **8.1** A plan for activity logs
- ✗ **8.2** Collect activity logs
- ✗ **8.3** Keep enough log storage
- ✓ **9.1** Supported web browsers and email apps only
- ✓ **9.2** DNS filtering (block known bad sites)
- ½ **10.1** Anti-malware on every device
- ½ **10.2** Automatic anti-malware updates
- ½ **10.3** Autorun off for USB drives
- ½ **11.1** A data recovery plan
- ✓ **11.2** Automatic backups
- ✗ **11.3** Protect the backups
- ✗ **11.4** Keep an isolated (offline / separate) backup copy
- ✓ **12.1** Keep network gear (router, firewall) up to date
- ✗ **14.1** A security awareness program
- ✗ **14.2** Training: spotting scams and phishing
- ✗ **14.3** Training: passwords and MFA
- ✗ **14.4** Training: handling data
- ✗ **14.5** Training: avoiding accidental leaks
- ✗ **14.6** Training: reporting incidents
- ✗ **14.7** Training: reporting missing updates
- ✗ **14.8** Training: risky Wi-Fi networks
- ✓ **15.1** Keep a list of service providers
- ✗ **17.1** Name who handles an incident
- ✗ **17.2** Keep incident contact numbers
- ✗ **17.3** A process for reporting incidents

This report lists what the owner told us and what anyone can see from outside (public DNS, the public homepage loaded once, certificate logs, spam blocklists, the domain registry). We did not log in anywhere, scan ports or test for weaknesses. It is not a security audit, a certification or insurance advice, and it doesn't promise coverage or a price: insurers' questions differ. Always answer an application truthfully: if the honest answer today is No, fix it first, then answer Yes. CIS Controls is a trademark of the Center for Internet Security; we are not affiliated.