SAMPLE | REDACTED | SECTIONS 1 · 2 · 4 · 5 · 6 · 9 · 10 · 12 · 13

Security & Compliance Evidence Pack

A plain-English security report — showing what was checked, what was found, and what it means for the business. No technical background needed to read this.

Business scanned: titanos.tech (our own infrastructure)
Date of scan: 24 June 2026
Prepared by: Kyle Deligny · **ABN:** 34 318 502 254
Report type: External security assessment — 8 of 13 sections shown

This is a sample of our own report — published so you can see the format before engaging.

The sections shown here are the externally-verifiable ones: the scan results, email security setup, website security, and the findings list. The sections that are specific to each client — your privacy policy, your breach response plan, your staff access record, your signed government checklist — are built from your own business data during the engagement. We don't include made-up versions of those in this sample because fabricating them would undermine the point.

What you're looking at: The same format, same structure, and same level of detail that every client receives — applied to our own business first.

01 — What we found: the summary

A plain-English overview of the check run on titanos.tech on 24 June 2026. Suitable for sharing with an insurer, a prospective enterprise client, or a regulator — no technical knowledge required to read it.

Overall result: Good posture, one minor item to fix.
Five items were checked. Four are in strong shape. One low-risk item (a missing certificate restriction record) is easy to fix and has been scheduled. No high-severity issues were found.

Area checked	Result	What it means in plain English
Website encryption	STRONG	All connections to the website use the strongest available encryption (same level as major banks). Customers and visitors are protected.
Email fraud protection	STRONG	Nobody can send a fake email pretending to be from this business. If they try, major email providers will reject it before it reaches anyone's inbox.
Protection against interception	STRONG	Browsers are locked to the secure version of the site. Even if someone tried to redirect visitors to an unsecured connection, it would fail.
Page security settings	PARTIAL	One browser security setting is applied through the page itself rather than at the server level — it works, but the more secure approach is to set it at the server. Scheduled for improvement.
Certificate restriction record	MISSING	No record tells the internet "only these certificate authorities are allowed to issue a security certificate for this domain." Low risk — easy to add. Scheduled.
Website access points	OK	The actual web server is protected behind Cloudflare and not directly visible on the internet. This is the correct setup.

02 — How this check was run

What we actually did — and what we deliberately did not do.

This is an **external, passive assessment** — meaning we ran the check from outside the business, looking at the same information that any attacker, enterprise client, or government agency would see when they look up your business online. We did not attempt to log in to anything, did not try to break anything, and did not access any private data.

> **In plain terms:** Think of this like a building inspector walking around the outside of your premises and checking the locks on the doors they can see from the street — not breaking in, not going through drawers. Everything in this report is visible to anyone with internet access.

What we checked:

- **Website connection security** — how your website encrypts data between itself and visitors
- **Email fraud protection** — whether your domain is set up to prevent fake emails
- **DNS records** — the internet's address book entries for your domain, which affect email security and certificate authority control
- **Security settings sent to browsers** — instructions your website gives to visitors' browsers about what it's allowed to do
- **What's publicly visible about your website's infrastructure** — what an attacker can see about how your site is hosted

Every finding in this report can be independently verified by anyone with internet access — we note what was checked and when, so anyone can re-run the same check and confirm the result.

> **90-day responsible disclosure:** For any significant finding identified during a client engagement, we notify the business and allow 90 days to fix it before publishing any reference to it. This sample contains only our own findings — we scan our own infrastructure and any domain we are explicitly authorised to scan.

04 — Your website and how it's accessed

We checked which "doors" to your website are open on the internet, who's answering them, and whether your actual web server is protected.

Connection point	Status	What this means
Standard web (port 80)	PROTECTED	Standard unencrypted web traffic — answered by Cloudflare (your web security provider), not your actual server. Cloudflare redirects all visitors to the secure version automatically.
Secure web (port 443)	PROTECTED	Encrypted web traffic (the "padlock" connection). Answered by Cloudflare. All visitor data travels over this encrypted connection.
Alternative ports (8080, 8443)	PROTECTED	Cloudflare's standard backup ports — also answered by Cloudflare, not your web server. Cloudflare blocks unauthorised requests on these automatically. No action needed.

Key finding: Your actual web server (hosted on GitHub Pages) is not directly visible on the internet from our vantage point. All traffic goes through Cloudflare first — this is the correct and secure configuration. An attacker cannot reach your web server directly; they have to go through Cloudflare's protections.

05 — Website encryption (the "padlock")

We verified the security certificate that protects all connections to the website.

What we checked	What we found
Certificate issued by	Google Trust Services — a major, publicly trusted certificate authority
Certificate covers	titanos.tech and all subdomains (e.g. api.titanos.tech)
Valid until	30 August 2026 — actively monitored; auto-renews on a 90-day cycle
Encryption strength	Strongest currently available standard — the same level used by major banks and government websites
Encryption version	TLS 1.3 — the current standard. Older, weaker versions are not accepted.
Browser lock-in (HSTS)	Active — browsers are permanently instructed to only use the secure version of this site, even if someone tries to redirect them to an unencrypted version. This setting is registered on a global browser preload list.
Certificate validation	Passed — independently confirmed as valid and not revoked

In plain terms: When someone visits titanos.tech, their connection is as secure as a visit to their online banking. The certificate is current, issued by a trusted authority, and uses the strongest available encryption. Browsers are locked to the secure version and cannot be tricked into using an unencrypted connection.

06 — Email fraud protection

We checked whether your domain is protected against email impersonation — one of the most common techniques used in invoice fraud and phishing attacks on small businesses.

> **Why this matters:** "Email spoofing" is when an attacker sends an email that appears to come from your business — your domain, your branding — but didn't. Common uses: fake invoices sent to your clients in your name, phishing emails to your staff pretending to be you, fraud. Three technical records (SPF, DKIM, DMARC) block this at the email provider level. If they're set correctly, major email providers like Gmail and Outlook will reject the fake email before it reaches anyone.

Protection	Status	What it does in plain English
SPF (Sender Policy Framework)	ACTIVE	A record that says "only Google's mail servers are authorised to send email from @titanos.tech." Anyone else trying to send as this domain will be rejected. Set to the strictest level.
DKIM (Email signing)	ACTIVE	A digital signature applied to every email sent from this domain. The recipient's email provider can verify the signature to confirm the email genuinely came from us and wasn't modified in transit.
DMARC (Fraud policy)	ACTIVE (strictest)	The overall policy that tells email providers what to do with emails that fail the checks above. Set to "reject" — meaning fake emails are blocked outright, not just flagged. We also receive a daily report of any attempts.
CAA record (Certificate restriction)	NOT SET	A record that restricts which certificate authorities are allowed to issue a security certificate for this domain. Currently absent — not a vulnerability, but a best-practice hardening step. Scheduled for addition. See finding F-01.

> **In plain terms:** The email fraud protection for titanos.tech is at the strongest practical configuration. If anyone tries to send a fake email from @titanos.tech, Gmail, Outlook, and most other major providers will reject it before it reaches the recipient. We also receive a daily report if any attempts are made.

09 — What you control vs what your provider controls

One of the most important things a compliance report clarifies: which security settings are yours to manage, and which ones are controlled by your hosting or technology providers. This matters because "reasonable steps" under Australian privacy law only applies to things you can actually control.

YOU CONTROL

- Your email security records (SPF, DKIM, DMARC) — set in your domain's DNS settings
- Your domain registrar account security (lock status, two-factor login)
- The security settings built into your website's code
- Your privacy policy content and the AI disclosure in it
- Who has access to your accounts and when that access is removed
- Your data breach response plan

YOUR HOSTING PROVIDER CONTROLS (CLOUDFLARE + GITHUB PAGES)

- The website's encrypted connection (the padlock)
- Protection against large-scale traffic attacks on the server
- Some browser security headers that need to be set at the server level
- Physical infrastructure and server-level hardening
- DDoS protection

Why this matters for your compliance: For any item in the "your provider controls" column, the compliance engagement gives you the exact language to send to your provider asking them to fix it. If they refuse or it's not possible, that refusal gets documented in your evidence pack as "reasonable steps taken" — which is the standard the regulator actually assesses against. You are never left responsible for something outside your control.

10 — What needs attention: findings list

Five items were logged from this scan. All are low-severity or informational — no urgent or high-risk issues were found. Listed in order of priority: easiest to fix with most benefit first.

F-01 No certificate restriction record published — LOW RISK

WHAT IT MEANS
Currently, any major certificate authority in the world could technically issue a security certificate for titanos.tech. A "CAA record" limits this to only the two providers that actually issue certificates for this domain. This doesn't create a current vulnerability — it just narrows the window for a rare type of attack involving a fraudulent certificate issued by a rogue authority.

REAL-WORLD IMPACT
Low. The specific attack this defends against requires a certificate authority itself to be compromised — an extremely rare event. But the fix takes 5 minutes and is best practice.

WHO FIXES IT
You — via your domain settings at Cloudflare (the DNS provider)

HOW HARD
5 minutes — add three lines to your DNS settings. Done on the working call.

STATUS
SCHEDULED — fix applied on working call

F-02 One browser security setting applied via the page, not the server — INFO — NO ACTION NEEDED

WHAT IT MEANS
A setting called "Content Security Policy" — which tells browsers what content is allowed to load on your pages — is currently set inside the page itself. This works correctly for visitors. The stricter approach is to have it set at the server level, so it applies even before the page loads. This is a best-practice improvement, not a current vulnerability.

REAL-WORLD IMPACT
None at present — the protection is working. This is an incremental hardening step.

WHO FIXES IT
Shared — the setting itself is ours; the server-level injection is a Cloudflare configuration

STATUS
INFORMATIONAL — scheduled for next infrastructure update

F-03 Browser permissions not explicitly declared

INFO — NO ACTION NEEDED

WHAT IT MEANS A "Permissions Policy" tells browsers which sensitive features — camera, microphone, location, payment — this website is allowed to use. Currently there's no explicit policy set. Since the site doesn't use any of those features, there's no current risk. Adding an explicit "deny all" policy guards against future changes accidentally enabling them.

REAL-WORLD IMPACT None today. Preventive measure for future-proofing.

WHO FIXES IT Hosting provider (Cloudflare) — a configuration-level change on their side

STATUS INFORMATIONAL — escalation language provided to Cloudflare

F-04 Two additional website access points visible

INFO — NO ACTION NEEDED

WHAT IT MEANS We can see four connection points to the website rather than the standard two. The extra two are Cloudflare's standard backup ports — they don't lead to your actual web server, and Cloudflare blocks any unauthorised requests on them automatically. Your actual server is not exposed through these.

REAL-WORLD IMPACT None — these are Cloudflare's default configuration. No origin server exposure.

WHO FIXES IT Not required. Cloudflare — optional stricter configuration available if desired.

STATUS INFORMATIONAL — no action required

F-05 Outdated browser instruction still being sent

INFO — NO ACTION NEEDED

WHAT IT MEANS The website sends an old security instruction ("Expect-CT") that was relevant a few years ago but has since been replaced by a new standard that all major certificate authorities now follow by default. Modern browsers simply ignore this instruction. It's not harmful — just a leftover from an older configuration that can be cleaned up.

REAL-WORLD IMPACT None. Deprecated instruction, ignored by current browsers.

WHO FIXES IT Hosting provider (Cloudflare) — optional cleanup item

STATUS INFORMATIONAL — no action required

12 — How to verify this independently

Every finding in this report is based on publicly accessible information. If you, your IT provider, or a prospective client wants to independently verify any claim, the information is available to anyone with internet access.

The checks run to produce this report use publicly available tools that can be run from any computer. They work by looking up publicly visible records on the internet — the same information any large enterprise client or government agency would check when doing due diligence on a supplier.

> **For your IT provider:** The raw technical output (the exact commands run and results returned) is available on request. Every finding can be independently reproduced from any internet-connected machine using standard tools. We provide the reproducibility commands to clients on the 30-day review call so your IT team can re-run the check themselves and confirm the current state.

What this means for your evidence pack: The value of a reproducible report is that any finding in it can be independently confirmed. If a regulator, insurer, or enterprise client questions a claim — "did you really fix the email fraud protection?" — you can point to a command they can run themselves to verify it. This is the difference between a document that says something was done and one that proves it.

13 — How this was produced and our commitment to you

What we scan:

- Our own infrastructure (this report)
- Any domain we are explicitly authorised to scan — every paying client engagement, plus businesses that have requested a free external scan via titanos.tech/scan

What we never do:

- Attempt to log in to anything
- Try to exploit any vulnerability
- Cause any disruption to the business being scanned
- Access private data

90-day responsible disclosure: For any significant finding identified during a client engagement, we notify the affected business and allow at least 90 days to fix the issue before making any public reference to it. This sample contains only findings from our own infrastructure.

About this sample: This document carries the same format, structure, and level of detail as every compliance engagement evidence pack — applied to our own business first. The sections not shown here (privacy policy, breach response plan, staff access record, Microsoft 365 / Google Workspace hardening evidence, two-factor login proof, backup plan, software update schedule, signed government security checklist, and privacy law compliance letter) are produced from each client's own business data during the engagement. We don't fabricate sample versions of those because a compliance document with made-up data defeats the purpose.

Kyle Deligny

ABN 34 318 502 254 · titanos.tech · kyle@titanos.tech

Every finding in this report is personally reviewed before it leaves our hands. The technical checks are run by automated tools, but the interpretation, the plain-English explanation, and the sign-off are mine. If something in this report is wrong, that's on me — and I give you the tools to check it yourself so you don't have to take my word for it.

Issued 2026-06-24. Re-issued with plain-English rewrite 2026-06-26. See titanos.tech/methodology for the full technical scope.