WEBSITE CONTENT SECURITY POLICY

CAPITAL GUARD
YOUR INVESTMENT SHIELD

Website Content Security Policy

Capital Guard AU Pty Ltd (AFSL 498434)
Issued by: Compliance Officer
Last Reviewed: 04/06/2025

---

1. Purpose and Scope

Capital Guard AU Pty Ltd ("Capital Guard", "we", "us", or "our") is committed to ensuring the confidentiality, integrity, and availability of its website content and related digital assets. This **Website Content Security Policy** outlines the technical and procedural safeguards in place to prevent unauthorised access, tampering, leakage, or disruption of any digital content or personal information made available via **www.capitalguard.com.au** ("the Website").

This Policy forms part of Capital Guard's broader cyber risk and compliance framework, and complements our:

- **Privacy Policy**,
- **Website Terms & Conditions**.

This Policy applies to all employees, contractors, third-party developers, hosting providers, and referrers who access, manage, or influence content hosted on the Website.

---

2. Legal and Regulatory Context

This Policy has been developed in accordance with:

- **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)**;
- **ASIC Report 429**: *Cyber resilience: Health check*;

- **ASIC's expectations for financial services licensees** under the **Corporations Act 2001 (Cth)** regarding system and data protection;
- **Australian Consumer Law**, in relation to representations made through online content;
- **ISO/IEC 27001** security principles (where adopted internally);
- **OWASP Top 10** vulnerabilities framework.

---

3. Content Integrity and Change Management

3.1 Controlled Access

All website content is maintained under version control. Changes to static or dynamic content (including disclosures, legal statements, financial service representations, and product descriptions) must be:

- Authorised in writing by the Compliance Officer;
- Logged and time-stamped;
- Reviewed for legal and factual accuracy;
- Deployed through secured CI/CD pipelines with staging validation.

3.2 Review and Approval

Any modification to the following content types must be subject to Compliance sign-off:

- Financial product statements;
- Fee or cost disclosures;

- Legal disclaimers and warnings;
- Terms & Conditions;
- Referrer and Remuneration Policies;
- Privacy-related consent language.

Unauthorized modifications will trigger an internal investigation and potential disciplinary measures.

---

4. Technical Safeguards

4.1 HTTPS and TLS Encryption

All content delivery is encrypted using **TLS 1.2 or higher**. Plain HTTP access is automatically redirected to HTTPS to ensure secure data transmission and content retrieval.

4.2 Content Security Policy (CSP) Headers

We enforce browser-level protection via the following HTTP headers:

- Content-Security-Policy: To control which domains are permitted to load scripts, images, fonts, and frames.
- X-Content-Type-Options: nosniff: To prevent MIME type sniffing.
- X-Frame-Options: DENY: To prevent clickjacking.
- Strict-Transport-Security: To enforce HSTS (HTTP Strict Transport Security).

Example CSP directive used:

csharp
CopyEdit

```
Content-Security-Policy:
default-src 'self';
script-src 'self' www.googletagmanager.com;
style-src 'self' 'unsafe-inline';
img-src 'self' data:;
frame-ancestors 'none';
form-action 'self';
```

4.3 Web Application Firewall (WAF)

All traffic to the Website is filtered through a Web Application Firewall, which:

- Blocks known malicious IP addresses;
- Detects and mitigates OWASP Top 10 attacks (e.g., XSS, SQLi, CSRF);
- Logs suspicious activity for compliance and incident review.

---

5. Authentication and Administrative Controls

- Admin interface is restricted to VPN-authenticated IP addresses.
- Two-Factor Authentication (2FA) is mandatory for administrative access.
- Access is role-based (RBAC), with least-privilege principles applied.
- Login attempts are rate-limited and logged for forensic purposes.

---

6. Hosting and Data Location

- The Website is hosted on a secure, ISO 27001-compliant cloud infrastructure.

- All data is stored in Australian-based data centres unless otherwise permitted under the Privacy Act and disclosed in our Privacy Policy.
- Backups are encrypted and maintained on a segregated environment with daily snapshots.

---

7. Monitoring, Logging, and Audit Trails

- Changes to content, metadata, and access credentials are logged with audit trails.
- Logs are retained in accordance with our Record Keeping Policy.
- Automated alerts are configured to notify Compliance and IT Security of:
    - Failed login attempts,
    - Unauthorised content changes,
    - Suspicious content injections.

Quarterly audits are performed to validate content integrity and control effectiveness.

---

8. Incident Management and Reporting

Any suspected or actual content breach, defacement, or data compromise triggers Capital Guard's **Incident Response Plan**, including:

- Immediate suspension of content publishing rights;
- Forensic capture of affected environment;
- Notification to the Compliance Officer and Director of IT Security;

- Determination of whether the breach constitutes a notifiable data breach under the **Privacy Act 1988 (Cth)**.

If required, affected individuals and regulators (including ASIC and the OAIC) will be notified in accordance with our breach notification protocol.

---

9. Third-Party Scripts, Plugins, and Integrations

Third-party integrations (e.g., analytics, payment APIs, chatbot services) are:

- Whitelisted by domain;
- Reviewed for privacy compliance and security exposure;
- Subject to contractual terms including breach notification and data handling controls.

No third-party script is embedded without Compliance review.

---

10. Public Communication and External Links

Capital Guard does not permit user-generated content. External links are reviewed for reputational and security risks prior to publication. All external links open in a new tab with rel="noopener noreferrer" to prevent cross-origin compromise.

Misuse of the Website or unauthorised reproduction of content is addressed in the Website Permission Policy.

---

11. Policy Governance and Review

This Policy is owned by the **Compliance Officer** and will be reviewed:

- At least annually;
- Immediately following any incident or regulatory development;
- Prior to the launch of any new digital product or online service channel.

Any deviations from this Policy must be approved in writing by the Board or the Managing Director.