

# Information Security *Policy*

Shockwave Media Pty Ltd · ABN 26 606 414 493 · Based in NSW, Australia

Version v1.0    Approved 8 October 2026    Effective 8 October 2026    Owner Managing Director  
Next review October 2027

## Document control

| VERSION      | DESCRIPTION                                                                                                                                                                                         | APPROVED BY                      | APPROVAL DATE  | EFFECTIVE DATE |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------|----------------|
| v1.0         | Initial release                                                                                                                                                                                     | Daniel Hooper, Managing Director | 8 October 2026 | 8 October 2026 |
|              |                                                                                                                                                                                                     |                                  |                |                |
| Policy owner | Daniel Hooper, Managing Director                                                                                                                                                                    |                                  |                |                |
| Applies to   | All Shockwave Media staff, contractors, systems, devices and services, and client systems and data we build, host or support, to the extent we are responsible for them under the relevant contract |                                  |                |                |
| Review       | Annually. Next review due October 2027, or earlier if law, contract requirements or our operations change materially.                                                                               |                                  |                |                |
| Published at | <a href="https://shockwavemedia.com.au/government/policies/">shockwavemedia.com.au/government/policies/</a>                                                                                         |                                  |                |                |

## 01 Purpose

This policy sets out how Shockwave Media Pty Ltd protects its own and its clients' information and systems. It aligns with ASD's Australian Cyber Security Centre (ASD's ACSC) Essential Eight and the Information Security Manual (ISM) where relevant, and with the supplier expectations in the NSW Cyber Security Policy, including incident notification and third-party risk management. Our control set is informed by ISO/IEC 27001:2022 and the ISM.

## 02 Governance

The Managing Director is accountable for information security. We keep a security risk register, review it quarterly, and report security risks and incidents to the Managing Director. All staff complete security awareness training at induction and annually, including phishing awareness.

## 03 Essential Eight

Our controls are aligned to ASD's Essential Eight mitigation strategies (patching applications and operating systems, multi-factor authentication, restricting administrative privileges, application control, Microsoft Office macro settings, user application hardening and regular backups), as set out in the sections below.

## 04 Access control and MFA

- ◆ Access is based on least privilege and need-to-know, approved by a team lead, and reviewed at least quarterly. Access is removed on the day a person leaves.
- ◆ Multi-factor authentication is required for email, source code repositories, cloud consoles, remote access and all systems holding client data. Phishing-resistant MFA is used where supported.
- ◆ Administrative accounts are separate from day-to-day accounts and limited to those who need them.
- ◆ Access to government client data is limited to Australian-based staff approved for that engagement.

## 05 Personnel and information handling

Staff assigned to government engagements are Australian-based, are bound by written confidentiality obligations, and complete national police checks or obtain security clearances where the client requires. We handle government information according to its classification and handling markings under the NSW Information Classification, Labelling and Handling Guidelines or the Commonwealth Protective Security Policy Framework. Security-classified (PROTECTED or above) information is handled only where the contract provides for it and an appropriately assessed environment is in place. At the end of an engagement, client data is returned or securely destroyed as the contract requires.

## 06 Devices and patching

Company devices are centrally managed, encrypted and have endpoint protection. Security patches for internet-facing services and critical vulnerabilities are applied within 48 hours where an exploit exists, and other patches within two weeks, in line with the Essential Eight. Unsupported software and operating systems are removed.

## 07 Secure software development

- ◆ All code changes are peer reviewed through pull requests before merging to protected main branches.
- ◆ Automated dependency scanning and secret scanning run on repositories, and static analysis is used where supported. Critical and high vulnerabilities are fixed before release, or risk-accepted in writing.
- ◆ We design against the OWASP Top 10 and apply OWASP ASVS controls appropriate to the risk of each system.
- ◆ Separate development, test and production environments are used. Production data is not used in non-production environments unless de-identified or approved by the client.
- ◆ Secrets are kept in managed secret stores, not in source code.

## 08 Encryption

Data is encrypted in transit using TLS 1.2 or higher and at rest using AES-256 or the cloud provider's equivalent managed encryption. Encryption keys are managed through the cloud provider's key management service with restricted access.

## 09 Hosting, backups and data sovereignty

Government client systems and data are hosted in Australian cloud regions. Backups are automated, encrypted, kept in Australia, protected from unauthorised change or deletion, and restore tests are carried out at least every six months. Backup frequency and retention are agreed with each client.

## 10 Logging and monitoring

Security-relevant events (authentication, privileged actions, configuration changes and application errors) are logged centrally, protected from tampering, and retained for at least 12 months or as the contract requires. Alerts are reviewed and acted on.

## 11 Incident response

- ◆ We maintain an incident response plan, an incident register, and test the plan at least annually.
- ◆ **We notify affected government clients of any suspected or actual security incident or data breach affecting their data or systems within 24 hours of becoming aware of it**, or sooner if the contract requires, and follow their reasonable directions during the investigation. This supports agencies' reporting to Cyber Security NSW and ASD's ACSC.
- ◆ We report incidents to ASD's ACSC where appropriate, meet Notifiable Data Breaches obligations under the Privacy Act, and meet any ransomware payment reporting obligations under the Cyber Security Act 2024 (Cth) that apply to us, including reporting to ASD within 72 hours.
- ◆ A post-incident review is carried out after every significant incident and lessons are fed back into controls.

## 12 Vendor management

We keep an inventory of the cloud, SaaS and other vendors that store or access client data. Before using a vendor for client data we assess its security (for example certifications, assurance reports and data location), and we review material vendors annually. For government engagements, vendors that store or process client data must host it in Australia unless the client agrees otherwise in writing.

## 13 AI system controls

For the AI systems we build, host or support (including LLM applications, agents, and retrieval-augmented generation (RAG) and knowledge systems), we apply these controls in addition to the rest of this policy. These controls support clients to meet the NSW AI Assessment Framework and AI Ethics Policy, and the Australian Government's Policy for the responsible use of AI in government, and they follow the National AI Centre's Guidance for AI Adoption.

- ◆ **Data isolation:** each client's data, prompts, embeddings and vector indexes, and logs are kept in separate, access-controlled environments. Client data is never shared between clients, never used to train models for anyone else or for our own purposes, and never made available to model providers for training. Where a client engages us to fine-tune a model on its data, that data and the resulting model stay in the client's environment and are used only for that client.
- ◆ **Model providers:** we use provider settings and terms that exclude client data from model training. For government data, models are used only through Australian-region deployments with in-region processing (no global or cross-region inference routing), or private models hosted in the client's Australian environment, with provider data retention minimised or disabled where available.
- ◆ **Prompt injection and untrusted content:** content retrieved from documents, websites, emails or tools is treated as untrusted. Inputs are screened using controls proportionate to the risk, and agents can call only allow-listed tools through least-privilege service accounts.
- ◆ **Data leakage:** retrieval is permission-aware, so it returns only sources the user is entitled to see, and outputs are checked for personal information and unsupported claims, automatically or by a person, in proportion to the risk of the use case.
- ◆ **Human review:** consequential actions, such as external communications, payments or changes to records, need approval by a person, with clear escalation paths.

- ◆ **Evaluation and monitoring:** test sets and acceptance criteria are agreed before release, regression tests run on every change, and production systems are monitored for quality, drift, cost and failure modes.
- ◆ **Audit logging:** prompts, sources, tool calls and approvals are logged under section 10, with personal information minimised and access restricted, subject to the client's retention requirements.
- ◆ **Model and data governance:** we document data flows (what is sent to which service, how long it is kept, and why), record the models and versions in use and each system's known limitations, and keep models behind an internal interface so a provider can be replaced.

## 14 Independent testing

We commit to annual independent penetration testing of our core infrastructure, and to testing client systems before go-live and after major changes where agreed with the client. Findings are tracked to resolution.

## 15 Business continuity

Information security is built into our business continuity and disaster recovery planning.

## 16 Compliance and review

Breaches of this policy may lead to disciplinary action. Where a client contract sets a stricter or different requirement, the contract prevails for that engagement. This policy is reviewed annually and after any significant incident. Based in NSW, Australia. Contact us via [shockwavemedia.com.au](https://shockwavemedia.com.au).

### Approval

Approved by Daniel Hooper, Managing Director, Shockwave Media Pty Ltd.

**Approval date:** 8 October 2026 · **Effective date:** 8 October 2026 · **Next review:** October 2027

**Signed:** Daniel Hooper (signed original held on file)