



Aussie Kohi

Security Policy

Disclaimer

This document has been prepared for educational purposes only. It forms part of a TAFE student assignment and describes a fictitious business that does not trade, take payment or ship goods.

The controls described here are the controls a small retailer of this kind would be expected to apply, and they are documented as a learning exercise rather than as a record of measures implemented on a live production system.

Nothing in this document is legal advice, and no reliance should be placed on it for any real commercial, legal or regulatory purpose. Any resemblance to a real business, person or transaction is unintended.

Document	Security Policy
Organisation	Aussie Kohi (aussiekohi.coffee)
Version	1.0
Effective date	3 September 2026
Review cycle	Annually, or sooner if the website or the law changes.
Owner	Website Owner, Aussie Kohi

This policy describes the controls applied to protect the Aussie Kohi website, the customer information it handles and the systems that support it. It is intentionally broad, and it is intended to sit alongside the Terms and Conditions and the Privacy Policy.

1. Purpose

The purpose of this policy is to protect the confidentiality, integrity and availability of the information held by Aussie Kohi, and to set a consistent baseline that anyone working on the website is expected to follow.

2. Scope

This policy covers the website and its source code, the hosting environment, the databases and backups, the business email accounts, the devices used to administer the site, and the third party services connected to it. It applies to the owner, to any staff or contractors, and to any student or volunteer contributing to the site.

3. Roles and responsibilities

Accountability is kept simple because the business is small, and responsibilities are allocated as follows:

- The Website Owner is accountable for this policy, for approving exceptions and for reviewing it annually.
- Anyone with administrative access is responsible for applying the controls described here in their day to day work.
- Third party providers are responsible for the security of the services they operate, as set out in their contracts.
- All users are responsible for reporting a suspected incident promptly.

4. Information classification

Information is classified so that effort is spent where it matters most. Three levels are used:

- Public information includes published product listings, brewing guides and blog articles, and it may be freely distributed.
- Internal information includes supplier pricing, draft content and system configuration, and it is shared only with those who need it.
- Confidential information includes customer personal information, order records and credentials, and it is protected by access control and encryption.

5. Access control

Access is granted on the principle of least privilege, so a user receives the minimum access needed to perform their role, and administrative access is limited to the smallest practical number of accounts. Accounts are individual rather than shared, so that activity can be attributed to a person.

Access is reviewed at least every six months, and access is revoked on the same day a person ceases to need it.

6. Authentication and passwords

Credentials are the most commonly attacked control, so the following requirements apply to every account used to administer or support the website:

- Passwords must be at least twelve characters long and must not be reused across services.
- Multi factor authentication must be enabled wherever the service supports it, including hosting, domain, email and payment accounts.

- Passwords must be stored in an approved password manager rather than in a browser, a spreadsheet or a note.
- Default credentials on any new system must be changed before that system is used.
- A credential that is suspected to be exposed must be changed immediately and the exposure reported.

7. Website and application security

The website accepts user input through the contact form and the cart, and input handling is therefore the primary application risk. The controls applied are set out below:

- All traffic is served over HTTPS using current transport layer security, and plain HTTP requests are redirected.
- All input is validated on the server as well as in the browser, because client side validation can be bypassed.
- Database queries use parameterised statements or prepared statements to prevent injection.
- Output is encoded before it is rendered, to prevent cross site scripting.
- Forms are protected against cross site request forgery and are rate limited to reduce automated abuse.
- Uploaded files are not accepted through public forms, and directory listing is disabled on the server.
- Error messages shown to users are generic, and detailed errors are written only to server logs.

8. Patching and change management

Unpatched software is a leading cause of compromise, so the content management system, libraries, server packages and plugins are kept current. Critical security patches are applied within seven days of release, and other patches are applied within thirty days.

Changes to the live site are tested before release, and a rollback path is identified before a significant change is made.

9. Payment security

Card data is handled entirely by the payment provider, and card numbers are never transmitted to, processed by or stored on our systems. Any provider used must maintain compliance with the Payment Card Industry Data Security Standard, and evidence of that compliance is obtained before the provider is engaged.

10. Data protection and encryption

Confidential information is encrypted in transit and at rest, and administrative devices use full disk encryption. Personal information is not copied to a local device, a personal email account or an unmanaged cloud drive.

Test and development environments use synthetic or de identified data rather than real customer records.

11. Backup and recovery

Backups protect against ransomware, hardware failure and human error, and they are only useful when they can be restored. The following applies:

- Website files and databases are backed up daily and retained for at least thirty days.
- At least one backup copy is held separately from the production environment.
- Backups are encrypted and access to them is restricted to administrators.
- A restore is tested at least every six months, and the result is recorded.

12. Logging and monitoring

Server, application and authentication logs are enabled and retained for at least ninety days, and they are reviewed for failed login attempts, unexpected administrative activity and unusual traffic patterns. Logs are protected from alteration, because a log that can be edited is not evidence.

13. Malware and endpoint protection

Devices used to administer the website run supported operating systems with automatic updates and reputable endpoint protection enabled. Software is installed only from trusted sources.

14. Physical security

Devices holding business information are locked when unattended, are not left visible in vehicles, and are password protected. Printed material containing personal information is stored securely and is shredded when no longer needed.

15. Third party and supplier security

Third parties introduce risk that we cannot directly control, so a provider is assessed before engagement for its security posture, its data location and its breach notification commitments. Access granted to a provider is limited to what the service requires and is removed when the engagement ends.

16. Acceptable use

Business accounts and systems are to be used for business purposes, and the following are prohibited:

- Sharing credentials with another person, including a colleague.
- Disabling or circumventing a security control without written approval.
- Connecting to administrative systems over an untrusted public network without a virtual private network.
- Installing unapproved software or browser extensions on an administrative device.
- Sending customer personal information to a personal email address or an unapproved messaging service.

17. Incident response

Early detection limits damage, so any suspected incident must be reported to the Website Owner immediately and must not be investigated informally. The response follows five steps:

- Identify the incident and record what is known, including the time it was detected.
- Contain the incident by isolating affected systems and revoking affected credentials.
- Eradicate the cause, including removing malicious code and closing the vulnerability used.
- Recover the service from a known good backup and confirm normal operation.
- Review the incident, record the lessons learned and update controls where a gap is found.

Where an incident involves personal information, the assessment and notification obligations under the Notifiable Data Breaches scheme are followed, as described in the Privacy Policy.

18. Vulnerability reporting

Reports of suspected vulnerabilities are welcomed and are treated as confidential. A report should be sent to the contact address published on the website and should describe the issue and the steps to reproduce it, and testing that degrades the service, accesses another person's data or modifies data is not authorised.

19. Training and awareness

Anyone with access to customer information is briefed on this policy before access is granted, and awareness of phishing, password hygiene and safe handling of personal information is refreshed at least annually.

20. Compliance and review

This policy supports our obligations under the Privacy Act 1988 (Cth) and reflects the intent of the Australian Cyber Security Centre Essential Eight guidance. It is reviewed annually, and it is reviewed sooner following a significant incident or a material change to the website.

A breach of this policy by a staff member or contractor may result in withdrawal of access and, where the breach is serious, termination of the engagement.

21. Contact

Questions, requests and complaints about this document may be directed to the contact details published on the website:

- Contact name is John Smith, Aussie Kohi.
- Postal address is 123A George Street, Perth, Western Australia 6000, Australia.
- Email address is the address published on the contact page of aussiekohi.coffee.
- Telephone number is the number published on the contact page of aussiekohi.coffee.

Because this is a student exercise, the contact details on the website are placeholders and are not monitored.