DIRECTORY.COM.AU PTY LTD

Web Development Quality Documentation

Aligned to Australian Standards

Document Reference: DCA-QMS-WEB-001
Version: 1.0
Issued: April 2026
Classification: Internal — Controlled

Document Control

Document Information

Attribute	Detail
Title	Web Development Quality Documentation
Document Reference	DCA-QMS-WEB-001
Version	1.0 (Initial Release)
Owner	Head of Engineering, Directory.com.au Pty Ltd
Approver	Chief Technology Officer
Classification	Internal — Controlled
Review Cycle	Annual, or upon material change to legislation, standards, or platform architecture
Next Review	April 2027

Revision History

Version	Date	Author	Summary of Changes
0.1	Mar 2026	Engineering Manager	Initial draft for internal review
0.9	Apr 2026	QA Lead	Incorporated WCAG 2.2 AA, ISO 27001:2023 and ACSC Essential Eight uplift
1.0	Apr 2026	Head of Engineering	Approved baseline release for company-wide adoption

Approvals

Role	Name	Date
Chief Technology Officer	_____	____ / ____ / _____
Head of Engineering	_____	____ / ____ / _____
Quality Assurance Lead	_____	____ / ____ / _____
Information Security Officer	_____	____ / ____ / _____

Table of Contents

This table of contents updates automatically. In Microsoft Word press F9, or right-click and select “Update Field”, to refresh page numbers after editing.

1. Executive Summary

Directory.com.au Pty Ltd (“the Company”, “Directory”) operates online directory and listings services that depend on secure, accessible, performant and lawful web platforms. This Quality Documentation defines the standards, processes and controls used by the Company’s web development function to plan, build, test, release and maintain web applications, websites and supporting APIs.

The framework set out in this document is aligned with Australian and internationally adopted standards including AS/NZS ISO 9001:2016 (Quality management systems), AS ISO/IEC/IEEE 12207:2018 (Software life cycle processes), AS/NZS ISO/IEC 25010:2017 (Systems and software quality models), AS/NZS ISO/IEC 27001:2023 (Information security management systems), AS/NZS ISO 31000:2018 (Risk management), the Web Content Accessibility Guidelines (WCAG) 2.2 Level AA, and the requirements of the Privacy Act 1988 (Cth) including the Australian Privacy Principles (APPs).

This document is mandatory reading for all engineering, quality, design, product and operations personnel involved in delivering web products at Directory.com.au. Compliance with this document is a condition of engagement for employees and contractors.

2. Purpose and Scope

2.1 Purpose

The purpose of this document is to:

- Establish a single, authoritative reference for web development quality at Directory.com.au Pty Ltd.
- Translate applicable Australian Standards, Commonwealth legislation and industry good practice into actionable engineering and quality controls.
- Define the minimum acceptable level of quality for any web product released to a Company environment, including production, staging and UAT.
- Provide an evidentiary basis for internal and external audits, due diligence, supplier assessment and customer assurance.

2.2 Scope

This document applies to all web-based information systems designed, built, hosted, integrated or maintained by, or on behalf of, Directory.com.au Pty Ltd. Specifically it covers:

- Public-facing websites and web applications, including the Directory.com.au consumer site and all subsidiary microsites.
- Authenticated member, advertiser and administrative portals.
- Backend services, REST and GraphQL APIs, and webhook integrations supporting the above products.
- Continuous integration and continuous deployment (CI/CD) pipelines, build tooling and infrastructure-as-code that produces or releases web artefacts.
- Third-party integrations, embedded widgets, and JavaScript supplied to external publishers under the Company’s brand.

2.3 Out of Scope

The following are governed by separate policies and are referenced where relevant: corporate IT (laptop fleet, identity), physical security, finance and procurement, marketing creative production, and any non-web product (for example native mobile binaries) where a separate Standard Operating Procedure exists.

2.4 Audience

Primary audience: software engineers, quality assurance engineers, site reliability engineers, product managers, designers and engineering managers. Secondary audience: information security, legal and compliance, customer support leadership, and executive sponsors.

3. Governing Standards and Regulatory Framework

Directory.com.au's web development practices map to the following standards and obligations. Where Standards Australia has adopted an ISO/IEC standard, the AS/NZS designation is authoritative.

3.1 Australian and Adopted International Standards

Reference	Title and Application
AS/NZS ISO 9001:2016	Quality management systems — Requirements. Provides the overarching QMS framework: leadership, risk-based thinking, process approach and continual improvement.
AS ISO/IEC/IEEE 12207:2018	Systems and software engineering — Software life cycle processes. Source of the SDLC phases used in Section 5.
AS/NZS ISO/IEC 25010:2017	Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models. Defines the eight quality characteristics used to assess web releases (functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability and portability).
AS/NZS ISO/IEC 27001:2023	Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Source of the ISMS controls referenced in Section 11.
AS/NZS ISO/IEC 27002:2022	Information security controls. Companion to ISO/IEC 27001 and used to design and operate the controls in Section 11.
AS/NZS ISO 31000:2018	Risk management — Guidelines. Underpins the risk-based prioritisation of testing, security and accessibility activity.
AS EN 301 549:2020	Accessibility requirements for ICT products and services. Adopted by the Digital Transformation Agency for Australian Government digital services and used here as a benchmark for procurement of third-party components.
WCAG 2.2 (W3C Recommendation)	Web Content Accessibility Guidelines. The Company targets Level AA conformance across all public web properties.

AS ISO/IEC 27701:2019	Privacy information management. Used to extend the ISMS to cover privacy obligations under the Privacy Act 1988 (Cth).
AS ISO 22301:2020	Business continuity management systems. Referenced for incident response, recovery objectives and continuity testing.

3.2 Australian Legislation and Regulator Guidance

Instrument	Relevance to Web Development
Privacy Act 1988 (Cth) and the Australian Privacy Principles	Collection, use, disclosure, storage and disposal of personal information; access and correction rights; cross-border disclosure; mandatory data breach notification under Part IIIC.
Notifiable Data Breaches scheme	Obligations to assess and notify the Office of the Australian Information Commissioner (OAIC) and affected individuals where an eligible data breach occurs.
Spam Act 2003 (Cth)	Consent, identification and unsubscribe requirements for commercial electronic messages sent by, or triggered from, the platform.
Disability Discrimination Act 1992 (Cth)	Underpins the Company's WCAG conformance commitments; informs the Australian Human Rights Commission's World Wide Web Access advisory note.
Australian Consumer Law (Schedule 2 to the Competition and Consumer Act 2010 (Cth))	Consumer guarantees, prohibition on misleading or deceptive conduct, and unfair contract terms — relevant to product copy, pricing displays and terms of use.
Security of Critical Infrastructure Act 2018 (Cth) and SOCI amendments	Where a Directory product is integrated into a critical infrastructure customer's environment, the Company will support the customer's obligations.
ACSC Information Security Manual (ISM) and Essential Eight	Australian Cyber Security Centre guidance forming the technical security baseline in Section 11.
DTA Digital Service Standard	Used as a benchmark for service design quality, even where the Company is not delivering to government.
Payment Card Industry Data Security Standard (PCI DSS) v4.0	Applies to any flow that stores, processes or transmits cardholder data; the Company's strategy is to remain SAQ-A by tokenising at the payment provider.

Where any standard or instrument is updated, the document Owner shall reassess this document within 60 calendar days and issue an amendment if required.

4. Quality Management System

The Company operates a Quality Management System (QMS) consistent with AS/NZS ISO 9001:2016. The QMS is process-based, risk-aware and oriented to continual improvement. This document forms part of the QMS for web development.

4.1 Quality Policy

Directory.com.au Pty Ltd is committed to delivering web services that are correct, accessible to all Australians, secure by design, respectful of personal information, and resilient under load. We commit to:

- Comply with applicable Australian legislation, regulatory guidance and adopted standards.
- Apply risk-based, evidence-led decision making across the software life cycle.
- Measure quality through agreed objectives and act on the results.
- Support our people with the training, tooling and time required to meet this standard.
- Continually improve the QMS through internal audit, customer feedback, post-incident learning and management review.

4.2 Quality Objectives

The Company sets, monitors and reports on the following objectives. Targets are reviewed annually.

Objective	Definition	Target
Defect Escape Rate	Production defects per 1,000 changed lines of code, by severity, measured monthly.	≤ 0.5 critical / ≤ 2.0 major
Change Failure Rate	Percentage of production deployments resulting in a rollback or hotfix within 24 hours.	≤ 10%
Mean Time to Restore (MTTR)	Mean elapsed time from incident detection to service restoration for Severity 1 and 2 incidents.	≤ 60 minutes (Sev 1)
Accessibility Conformance	Automated and manual WCAG 2.2 AA conformance score across audited pages.	≥ 95% pass rate
Security Posture	Open critical and high vulnerabilities older than the SLA in Section 11.	0 open beyond SLA
Customer Satisfaction	Quarterly Net Promoter Score across product surfaces.	≥ +30

4.3 Document and Records Control

All QMS documents are version-controlled in the corporate documentation system. Engineering artefacts (source code, build logs, test results, evidence of approvals, deployment records) are retained for at least seven years for tax and regulatory purposes, and longer where contractual or legislative obligations require it. Records of personal information handling are retained in accordance with the Company's Privacy Policy and the Australian Privacy Principles.

4.4 Management Review

The Quality Forum (chaired by the CTO) meets at least quarterly to review performance against the objectives in Section 4.2, the status of internal audit findings, customer complaints, security and privacy incidents, and improvement opportunities. Meeting outcomes are minuted and tracked to closure.

5. Software Development Lifecycle

Directory.com.au follows an iterative, agile delivery model that conforms to the process areas of AS ISO/IEC/IEEE 12207:2018. The lifecycle is divided into the phases below. Smaller changes (for example a copy fix) may compress phases but cannot omit any quality gate marked Mandatory.

5.1 Lifecycle Phases and Gates

Phase	Activities	Quality Gate (Mandatory unless noted)
Discovery	Problem definition, user research, success metrics, regulatory screen, accessibility and privacy first-pass assessment.	Discovery brief approved by Product and Engineering Lead.
Design	Solution design, data flow diagrams, threat modelling (STRIDE), Privacy Impact Assessment trigger check, accessibility review of designs.	Design Record signed off; threat model recorded; PIA completed where personal information is in scope.
Build	Implementation against acceptance criteria; unit tests; static analysis; secrets and dependency scanning.	All pull requests pass CI; minimum two reviewer approvals; coverage thresholds met.
Verify	Integration, end-to-end, accessibility, performance, security, regression and exploratory testing.	Test Summary Report signed off by QA Lead; risk-accepted defects recorded.
Release	Change Advisory review, production deployment using progressive delivery, smoke tests, observability check.	Change record approved; rollback verified; on-call rota notified.
Operate	Monitoring, alerting, on-call response, incident management, customer support triage.	SLOs met; incident reviews completed within 5 business days.
Improve	Retrospectives, defect trend analysis, performance and security baselining, training updates.	Improvement actions logged with owner and due date.

5.2 Definition of Ready

A backlog item is ready for build when all of the following are true:

- Independent business value is articulated and linked to a measurable outcome.
- Acceptance criteria are testable and written in user-facing language.

- Non-functional requirements (performance, accessibility, security, privacy, observability) are explicit.
- Dependencies, data sources and external services are identified.
- The item is sized and within sprint capacity.

5.3 Definition of Done

A change is done when:

- Code is merged to the protected main branch via a reviewed pull request.
- All automated checks (unit, integration, accessibility, security, lint) are green.
- Manual test evidence (where required) is attached to the work item.
- Documentation, including operational runbooks where applicable, is updated in the same release.
- The change is deployed to production or scheduled for the next release window.
- Telemetry, dashboards and alerts reflect the new behaviour.

6. Coding Standards and Conventions

6.1 Principles

Code authored at Directory.com.au is read more often than it is written. Authors prefer clarity over cleverness, consistency over local optima, and small, reversible steps over large, irreversible ones.

- Favour explicit over implicit behaviour; avoid hidden side effects.
- Treat all input as untrusted until validated.
- Apply the principle of least privilege to data, network and process boundaries.
- Optimise only after measuring; document any non-obvious optimisation.
- Write code that is testable in isolation and observable in production.

6.2 Language and Framework Standards

Stack	Standard
HTML5	Semantic, valid HTML conforming to the WHATWG Living Standard. Documents must declare a language attribute and use landmark elements (header, main, nav, footer).
CSS / Sass	BEM or utility-first conventions; design tokens sourced from the Directory Design System; no inline styles in production templates.
JavaScript / TypeScript	TypeScript strict mode; ESLint with the Company’s shared config; Prettier for formatting; no use of any without a documented exception.
Node.js services	Active LTS only; structured logging; graceful shutdown; readiness and liveness endpoints.
PHP services	Supported PHP version per the official PHP support policy; PSR-12 coding style; PHPStan level ≥ 6.

APIs	REST APIs follow the Company API Style Guide; OpenAPI 3.1 specification per service; semantic versioning of public endpoints.
SQL	Parameterised queries only; no string concatenation of user input into SQL; explicit transactions for multi-statement writes.

6.3 Naming, Comments and Structure

- Files, modules and functions named in domain language; abbreviations only when industry-standard.
- Public functions, exported types and complex algorithms carry a doc comment explaining intent, inputs, outputs and side effects.
- TODO and FIXME comments include an author handle and a tracking ticket reference.
- Dead code is deleted, not commented out; version control retains history.

6.4 Internationalisation and Localisation

All user-facing strings are externalised. The Company's primary locale is en-AU; Australian English spelling and date formats (DD/MM/YYYY) are used unless an upstream system imposes another format. Currency is displayed as AUD with the dollar symbol and a space ("$ 1,234.50" is acceptable; the placement must be consistent within a screen).

7. Version Control and Source Code Management

All source code, infrastructure-as-code and engineering documentation are stored in the Company's Git platform. Local-only repositories or untracked code are not permitted.

7.1 Branching Model

The Company uses trunk-based development with short-lived feature branches:

- main is always deployable. Direct pushes are blocked.
- Feature branches are named feat/<ticket>-<short-slug>, and merged via pull request within 3 working days where possible.
- Hotfix branches are named hotfix/<ticket>-<short-slug> and may target a release tag.
- Release tags follow Semantic Versioning 2.0.0 (MAJOR.MINOR.PATCH).

7.2 Commit Discipline

- Commit messages use Conventional Commits (e.g. feat:, fix:, chore:) and reference the work item ID.
- Commits are scoped: one logical change per commit; refactors separate from behavioural change.
- Force-pushes to shared branches are forbidden; rebasing is permitted on private feature branches.

7.3 Branch Protection

Repositories that produce production artefacts must enforce:

- Mandatory pull request review by at least two engineers (one outside the immediate squad for high-risk repositories).
- Required CI checks (build, lint, unit, integration, accessibility, dependency and secrets scans).
- Signed commits or signed tags for release artefacts.
- Linear history (no merge commits into main).

8. Code Review

Code review is the principal control for engineering quality and a key information-sharing mechanism. Reviews are conducted respectfully, in writing, and with the codebase as the source of truth.

8.1 Reviewer Checklist

- The change does what the work item describes, and only that.
- Behaviour is covered by automated tests at the appropriate layer.
- Failure modes are handled; user-facing errors are accessible and actionable.
- No personal information appears in logs, error messages or test fixtures.
- Inputs are validated; outputs are encoded appropriately for their context (HTML, URL, JSON, SQL).
- Secrets, credentials, internal hostnames and customer data are absent from the diff.
- Dependencies introduced are licensed compatibly and assessed for supply-chain risk.
- The change has a rollback plan, or is feature-flagged.

8.2 Review Service Levels

- First reviewer responds within 1 working day.
- Pull requests are merged within 3 working days of opening, or explicitly paused.
- Critical security or production fixes are reviewed within 2 hours during business hours and within 4 hours outside.

9. Testing and Quality Assurance

Testing is risk-based and layered. The Company applies the practical test pyramid: many fast unit tests, fewer integration tests, and a curated set of end-to-end tests covering critical user journeys.

9.1 Test Levels

Level	Purpose	Minimum Standard
Unit	Verify behaviour of an isolated module without external dependencies.	≥ 80% line coverage on changed code; mutation score reported quarterly.
Integration	Verify interaction between components, including database, queue and HTTP boundaries.	Critical paths covered; runs in CI on every pull request.

Contract	Verify provider-consumer compatibility for internal and external APIs.	Consumer-driven contracts published for every public endpoint.
End-to-end	Verify critical user journeys in a production-like environment.	Smoke and journey suites green before and after every production release.
Accessibility	Verify WCAG 2.2 AA conformance across pages and components.	Automated checks on every PR; manual audit of new flows; see Section 10.
Performance	Verify response time, throughput and resource usage targets.	Load tests for every revenue-critical surface; budgets in CI; see Section 13.
Security	Static, dynamic and dependency analysis; penetration testing.	SAST/DAST in CI; annual external pentest; see Section 11.
Exploratory	Risk-based, time-boxed manual investigation.	Charter recorded; findings logged as defects with reproduction steps.

9.2 Defect Severity and Service Levels

Severity	Definition	Target Resolution
S1 — Critical	Major outage, data loss, security breach, payment failure or accessibility blocker preventing use of a core journey.	Mitigated within 60 minutes; permanently resolved within 24 hours.
S2 — High	Significant impairment of an important journey with no acceptable workaround.	Resolved within 5 business days.
S3 — Medium	Defect with workaround or affecting a non-critical journey.	Resolved within the next minor release.
S4 — Low	Cosmetic, copy or minor usability issue.	Triaged into the backlog.

9.3 Test Data Management

- Production personal information is not used in non-production environments.
- Synthetic or de-identified datasets are generated from a controlled fixtures library.
- Where production-like data is unavoidable (for example a one-off defect investigation), access is time-bound, logged, and approved by the Information Security Officer.

10. Accessibility

Accessibility is a non-negotiable quality attribute. The Disability Discrimination Act 1992 (Cth) prohibits discrimination in the provision of goods and services, and the Australian Human Rights Commission expects organisations to apply WCAG to web content.

Directory.com.au targets Web Content Accessibility Guidelines (WCAG) 2.2 Level AA across all public web properties.

10.1 Conformance Targets

- All new and substantially redesigned public pages: WCAG 2.2 AA at release.
- Authenticated user-facing tools: WCAG 2.2 AA progressively, prioritised by usage.
- Internal tools: WCAG 2.1 AA where practicable.
- Procured third-party components must provide an Accessibility Conformance Report (ACR) that is reviewed during vendor assessment.

10.2 Practices

- Designers produce annotated specifications including heading hierarchy, focus order, error states and reduced-motion variants.
- Engineers prefer native HTML semantics; ARIA is used only where native semantics are insufficient.
- Colour contrast meets at least 4.5:1 for body text and 3:1 for large text and meaningful non-text content.
- Interactive components are operable by keyboard, screen reader and voice control; focus indicators are clearly visible.
- Forms include labels, instructions, accessible error messaging, and respect autocomplete tokens.
- Media includes captions; transcripts are provided for prerecorded audio.

10.3 Testing and Audit

- Automated checks (axe-core or equivalent) execute on every pull request; failing rules block merge.
- Manual conformance audits are performed quarterly by the QA Accessibility Champion using the W3C ACT Rules and assistive technologies (NVDA, VoiceOver, TalkBack, Dragon).
- An external accessibility audit is commissioned at least annually for the consumer site.
- User feedback channels include an accessible mechanism for reporting accessibility issues, monitored by Customer Support.

11. Information Security

The Company’s Information Security Management System (ISMS) is designed in accordance with AS/NZS ISO/IEC 27001:2023 and operationalised using AS/NZS ISO/IEC 27002:2022 controls and the Australian Cyber Security Centre’s Information Security Manual (ISM) and Essential Eight.

11.1 Secure Development Lifecycle Activities

- Threat modelling using STRIDE for any change that introduces a new trust boundary, data class or external integration.

- Static Application Security Testing (SAST) on every pull request; findings categorised against OWASP ASVS Level 2.
- Software Composition Analysis (SCA) and Software Bill of Materials (SBOM) generation per build.
- Dynamic Application Security Testing (DAST) on staging for revenue-critical services.
- Secrets scanning on every commit; rotated keys for any leak, with post-incident review.
- Annual independent penetration test of the consumer site and authenticated portals.

11.2 Web Application Controls

- OWASP Top 10 mitigations are baseline; the OWASP Application Security Verification Standard (ASVS) is the gold standard.
- All traffic is served over TLS 1.2 or 1.3 with HSTS enabled; insecure cipher suites are disabled.
- HTTP security headers (Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, X-Frame-Options or frame-ancestors) are mandatory and tested.
- Authentication uses industry-standard protocols (OAuth 2.1 / OIDC); passwords stored using a memory-hard hash; MFA is required for staff and offered to consumers.
- Sessions are bound to the user agent, expire on inactivity, and are invalidated on credential change.
- Output encoding is context-aware to prevent XSS; CSRF protections apply to state-changing requests.
- Rate limiting and bot mitigation protect public endpoints.

11.3 Vulnerability Management Service Levels

Severity (CVSS v3.1)	Examples	Remediation Target
Critical (≥ 9.0)	RCE, auth bypass, exposure of bulk personal information.	Mitigated within 24 hours; resolved within 7 days.
High (7.0–8.9)	Privilege escalation, exploitable XSS, sensitive information disclosure.	Resolved within 30 days.
Medium (4.0–6.9)	Lower-impact misconfigurations, outdated dependencies without active exploit.	Resolved within 90 days.
Low (< 4.0)	Hardening recommendations.	Tracked and resolved opportunistically.

11.4 Essential Eight Alignment

The Company tracks maturity against the ACSC Essential Eight (application control, patch applications, configure Microsoft Office macro settings, user application hardening, restrict administrative privileges, patch operating systems, multi-factor authentication, regular

backups). Web development inherits these controls from the corporate IT environment and supplements them with web-specific controls in 11.2.

12. Privacy and Data Protection

Directory.com.au handles personal information of consumers and business customers. The Company complies with the Privacy Act 1988 (Cth) and the thirteen Australian Privacy Principles (APPs), and operates a privacy management programme that aligns with AS ISO/IEC 27701:2019.

12.1 Privacy by Design

- Privacy is considered at Discovery and Design phases; a Privacy Impact Assessment (PIA) is completed for any new collection or use of personal information.
- Data minimisation: only the personal information necessary for a documented purpose is collected; default form fields do not include unnecessary identifiers.
- Purpose binding: personal information is used or disclosed only for the primary purpose disclosed at collection, or a related secondary purpose the individual would reasonably expect.
- Retention: personal information is retained only for as long as required for the purpose, or by law, after which it is securely destroyed or de-identified.

12.2 Engineering Practices

- Personal information is encrypted in transit (TLS 1.2/1.3) and at rest (AES-256 or platform-equivalent).
- Production datastores are segmented from development and staging.
- Access to personal information follows the principle of least privilege; access is logged and reviewed quarterly.
- Cookie banners and consent mechanisms reflect Australian regulatory expectations and any applicable foreign law for international audiences.
- Data subject access and correction requests are routed to a defined queue with a 30-day SLA, consistent with APP 12 and APP 13.

12.3 Notifiable Data Breaches

If the Company forms a reasonable belief that an eligible data breach has occurred, the Information Security Officer assesses the incident within 30 days. Where required, the Office of the Australian Information Commissioner and affected individuals are notified as soon as practicable in accordance with Part IIIC of the Privacy Act 1988 (Cth). Engineers must report any suspected data exposure to the security on-call channel immediately.

12.4 Cross-Border Disclosure

Where personal information is disclosed to an overseas recipient (for example a cloud or analytics vendor), the Company takes reasonable steps to ensure the recipient does not breach the APPs, consistent with APP 8. Vendor assessments record the country of processing and the contractual safeguards in place.

13. Performance, Compatibility and Reliability

Performance is treated as an accessibility and usability concern. The Company applies budgets and tests them in CI.

13.1 Core Web Vitals Targets

Metric	Definition	Target (75th percentile, mobile)
Largest Contentful Paint	Loading performance — time to render the largest visible element.	≤ 2.5 seconds
Interaction to Next Paint	Responsiveness to user input.	≤ 200 milliseconds
Cumulative Layout Shift	Visual stability — unexpected layout movement.	≤ 0.1
Time to First Byte	Server response time.	≤ 800 milliseconds

13.2 Browser and Device Support

The Company supports the latest two major versions of Chrome, Edge, Firefox and Safari on Windows, macOS, iOS and Android. Progressive enhancement ensures that core content remains accessible to older user agents.

13.3 Reliability Objectives

- Service Level Objective (SLO) for the consumer site: 99.9% monthly availability.
- Recovery Time Objective (RTO): 1 hour for Tier 1 services.
- Recovery Point Objective (RPO): 15 minutes for transactional data.
- Backups are tested by restore at least quarterly; results are recorded.

14. Deployment and Release Management

Releases are progressive, observable and reversible.

- Production deployments use blue/green or canary patterns; feature flags decouple deployment from release.
- Every change has a documented rollback procedure that has been verified in a non-production environment.
- Release windows avoid Friday afternoons, public holidays and high-traffic events unless a Severity 1 fix requires it.
- Build artefacts are immutable, signed, and stored in the Company artefact registry with retention aligned to records-keeping requirements.
- Infrastructure changes follow the same review and gating standards as application code.
- Production access is granted just-in-time via approved automation and is logged.

15. Operations, Monitoring and Incident Management

15.1 Observability

- Every service emits structured logs, metrics and traces in line with the Company's observability standard.
- Service-level indicators (SLIs) and SLOs are defined per service, with error budgets visible to the squad.
- Alerts are actionable, routed to the on-call rota, and reviewed monthly to suppress noise.

15.2 Incident Management

Incidents follow a five-step lifecycle: detect, declare, respond, restore, review. The Incident Commander coordinates the response; an Engineering Lead drives technical actions; a Communications Lead handles internal and external messaging where required.

- All Severity 1 incidents trigger a blameless post-incident review within 5 business days.
- Reviews produce action items with owners and due dates, tracked to closure.
- Where personal information may be affected, the Information Security Officer triggers the Notifiable Data Breach process (Section 12.3).

16. Documentation Requirements

Documentation is a deliverable, not an afterthought. Every production service must maintain:

- A README in the repository describing purpose, ownership, local development and links to deeper documents.
- An Architecture Decision Record (ADR) log capturing significant decisions and their context.
- An OpenAPI specification (for HTTP services) kept in sync with the implementation.
- A runbook covering common operational tasks, alert responses and escalation paths.
- A data dictionary identifying personal information and any regulated data classes.
- User-facing release notes for changes affecting customers.

17. Roles, Responsibilities and Training

17.1 RACI Summary

Activity	CTO	Eng. Lead	QA Lead	InfoSec Officer
Quality policy ownership	A	R	C	C
Threat modelling	I	R	C	A
Test strategy	I	C	A/R	C
Accessibility audit	I	C	A/R	I
Vulnerability remediation	I	R	C	A

Privacy impact assessment	I	R	C	A
Incident command	I	A/R	C	C

R = Responsible; A = Accountable; C = Consulted; I = Informed.

17.2 Training

- All engineers complete onboarding training covering this document, the Privacy Act and APPs, secure coding, and accessibility within 30 days of starting.
- Annual refreshers cover changes to legislation, standards and the Company threat landscape.
- Specialist roles (security champions, accessibility champions) attend additional, role-specific training each year.

18. Compliance, Audit and Continual Improvement

- Internal audit reviews this document and a sample of releases at least annually; findings are tracked to closure by the Quality Forum.
- External attestations (for example SOC 2 Type II or ISO 27001 certification) are pursued in line with the Company's commercial roadmap.
- Customer audit requests are coordinated by the Information Security Officer.
- Improvement opportunities can be raised by any employee via the Quality Improvement register; the Quality Forum prioritises them quarterly.

19. Glossary

Term	Definition
ACSC	Australian Cyber Security Centre, the Australian Government's lead cyber security agency.
APP	Australian Privacy Principle. Thirteen principles in Schedule 1 to the Privacy Act 1988 (Cth).
ASVS	OWASP Application Security Verification Standard, used as the gold-standard security baseline.
CI/CD	Continuous Integration / Continuous Deployment.
DAST	Dynamic Application Security Testing — black-box scanning of running applications.
ISMS	Information Security Management System per AS/NZS ISO/IEC 27001:2023.
ISM	Information Security Manual published by the ACSC.
OAIC	Office of the Australian Information Commissioner.

PIA	Privacy Impact Assessment.
RTO / RPO	Recovery Time Objective / Recovery Point Objective.
SAST	Static Application Security Testing — white-box analysis of source or compiled code.
SBOM	Software Bill of Materials.
SDLC	Software Development Lifecycle.
SLO / SLI	Service Level Objective / Indicator.
WCAG	Web Content Accessibility Guidelines published by the W3C.

20. References

- Standards Australia, AS/NZS ISO 9001:2016 — Quality management systems — Requirements.
- Standards Australia, AS ISO/IEC/IEEE 12207:2018 — Software life cycle processes.
- Standards Australia, AS/NZS ISO/IEC 25010:2017 — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models.
- Standards Australia, AS/NZS ISO/IEC 27001:2023 — Information security management systems — Requirements.
- Standards Australia, AS/NZS ISO/IEC 27002:2022 — Information security controls.
- Standards Australia, AS/NZS ISO 31000:2018 — Risk management — Guidelines.
- Standards Australia, AS EN 301 549:2020 — Accessibility requirements for ICT products and services.
- World Wide Web Consortium (W3C), Web Content Accessibility Guidelines (WCAG) 2.2.
- Privacy Act 1988 (Cth) and the Australian Privacy Principles.
- Office of the Australian Information Commissioner, Notifiable Data Breaches scheme guidance.
- Spam Act 2003 (Cth).
- Disability Discrimination Act 1992 (Cth) and the Australian Human Rights Commission, World Wide Web Access: Disability Discrimination Act Advisory Notes.
- Australian Consumer Law (Schedule 2 to the Competition and Consumer Act 2010 (Cth)).
- Australian Cyber Security Centre, Information Security Manual; Essential Eight Maturity Model.
- Digital Transformation Agency, Digital Service Standard.
- OWASP Foundation, OWASP Top 10 and Application Security Verification Standard.
- PCI Security Standards Council, PCI DSS v4.0.

End of document.