CredEntry

Powered by

APPENDIX E

SUPPORT AND MAINTENANCE FRAMEWORK

Table of Contents

1. Purpose and Scope

This section outlines the intent of the Support & Maintenance Framework, ensuring all obligations under Schedules 2, 3, 5 and 6 are addressed. It defines how CredEntry will deliver comprehensive support, training, onboarding, incident management, reporting, and lifecycle coverage across the Digital Wallet Solution.

*(See also **Appendix I – Standards Compliance Mapping, Appendix A – SLA**)*

Our Support and Maintenance Framework provides a complete service model for the ongoing operation of the Digital Wallet and Verifiable Credentials Solution. It demonstrates how we will ensure service reliability, protect citizen trust, and meet all contractual obligations under Schedule 5 – Ongoing Services and Schedule 6 – Performance Assessment Regime.

The framework covers support delivery, incident and vulnerability management, system performance, governance and reporting, and resilience planning, and is underpinned by our Service Level Agreement (SLA) and Business Continuity & Disaster Recovery Plan (BCP/DRP).

2. Support Services

This section describes the day-to-day support services available to citizens, agencies, and integration partners. It covers the service desk model, hours of operation, escalation channels, and ongoing updates.

*(See also **Appendix A – SLA, Appendix E – Communications Templates & Escalation Contacts**)*

- **Citizens:** Access to wallet support through in-app help, FAQs, and knowledge base.
- **Agencies and Administrators:** WA-based service desk (8:00am–5:00pm AWST) with direct access to support specialists for credential, issuance, or revocation queries.
- **Emergency Escalation:** 24/7 coverage for Severity 1 incidents ensures continuity of critical services such as verification and revocation.
- **Developers and Integration Partners:** Access to SDK documentation, technical support, and integration assistance via structured DevOps workflows.

3. Service Levels and Availability

This section establishes the service performance targets for availability, recovery, and resilience, backed by monitoring and reporting mechanisms. It demonstrates alignment with WA Government’s uptime and continuity requirements.

*(See also **Appendix A – SLA, Appendix F – Testing Results & Improvement Log**)*

- **Availability Commitments:** 99.95% uptime for credential verification and revocation; 99.90% for issuance and APIs; 99.80% for admin dashboard.
- **Resilience Design:** Active-active Azure deployment across sovereign regions, with automated failover and RTO/RPO targets of 2–4 hours / 15–30 minutes.
- **Monitoring and Fraud Detection:** Continuous monitoring via Azure Sentinel, Event Hubs, and Redis caching. Real-time anomaly alerts protect against fraudulent credential activity.

- **Performance Visibility:** Administrators access a secure dashboard with live performance, audit logs, and compliance reporting.

4. Training Plan

This section describes the structured training program to ensure WA Government staff and stakeholders are fully equipped to operate and administer the Digital Wallet. It outlines training content, delivery, and evaluation methods.

(See also ***Appendix B – Training Plan, Appendix C – Release & Onboarding Process Flow****)*

CredEntry will deliver a structured training methodology covering:

- Training delivered at least four weeks prior to Pilot commencement.
- Role-based training for administrators, developers, and support staff.
- Integration into a Knowledge Management Database to maintain policies and procedures.
- Post-training evaluation to measure effectiveness and adoption.

5. Onboarding & Implementation Support

This section covers the onboarding of administrators, issuers, and citizens during Proof-of-Operation, Pilot, and Production phases. It ensures a smooth transition with detailed documentation, guides, and direct support.

(See also ***Appendix C – Release & Onboarding Process Flow, Appendix E – Communications Templates****)*

- End-to-end support for Proof-of-Operation, Pilot Phase, and Production transition.
- Administrator onboarding and credential provider enablement.
- Documentation including admin guides, SDK integration materials, and sample credential workflows.
- Supplier and stakeholder engagement as required by DGov.

6. Maintenance and Continuous Improvement

This section sets out how planned, emergency, and ongoing maintenance activities are conducted, with a focus on service continuity, product enhancement, and warranty coverage. It demonstrates the continuous improvement culture underpinning the solution.

(See also ***Appendix F – Testing Results & Improvement Log, Appendix J – Warranty Inclusions & Exclusions****)*

- **Planned Maintenance:** Scheduled outside business hours, ≤4 hrs/month, ≥7 days’ notice.
- **Emergency Maintenance:** Executed as required with immediate Department notification.
- **Change & Release Management:** ITIL v4 processes to introduce patches, features, and updates without disruption.
- **Product Roadmap:** Future-proofed enhancements (e.g. biometrics, interoperability modules) delivered through structured release cycles and agreed roadmaps.

6A. Service Lifecycle Coverage

This section demonstrates CredEntry's ability to provide support across the full service lifecycle — from Proof-of-Operation and Pilot to Production and Transition-Out — ensuring continuity at every stage.

*(See also **Appendix G – BCP & DRP, Appendix H – Recovery Runbooks & Checklists**)*

- **Proof-of-Operation** – Dedicated support during integration and demonstration activities, including technical walkthroughs, SDK guidance, and incident capture aligned to evaluation requirements.
- **Pilot Phase** – Tiered support for restricted and preview pilots, structured reporting of issues, and targeted training cycles. Dedicated resources ensure continuity as the wallet scales to live users.
- **Production Operation** – Full SLA-backed support services, incident management, vulnerability scanning, performance monitoring, and ongoing training.
- **Transition-Out** – In line with the Agreement (clause 58), CredEntry will provide structured transition-out support, including data handover, runbooks, documentation, and knowledge transfer to ensure continuity of government services.

6B. Stakeholder Engagement & Service Lifecycle

This section outlines the key stakeholders in the Digital Wallet ecosystem, their roles and responsibilities, and the engagement models CredEntry maintains to ensure effective collaboration and support.

*(See also **Appendix D – Reporting Matrix, Appendix E – Communications Templates**)*

Stakeholder	Role & Responsibilities	Engagement Model
Office of Digital Government (DGov)	Contract owner; defines requirements; governs service; manages DTP and IdX	Weekly steering committee
ServiceWA & Adapptor	Owns ServiceWA app; integrates SDK; manages UX	Daily stand-ups during integration
Digital Wallet Provider (CredEntry)	Develops and operates platform; provides SDKs; ensures compliance and service continuity	Dedicated Account Manager
Credential Issuers (Agencies)	Provide credentials via DTP; maintain attribute sources	Monthly issuer forums
Citizens	Hold credentials; consent to usage; recover wallets via in-app support	ServiceWA integrated support
Verifiers & Relying Parties	Accept credentials; validate proofs	Developer portal access and technical documentation
WA Identity Exchange (IdX)	Provides federated authentication for wallets and relying parties	Technical integration team collaboration

7. Incident Management & Escalation

This section defines how incidents are categorised, escalated, and resolved, including severity levels, PIR requirements, and escalation pathways. It ensures alignment with WA Government security and continuity requirements.

*(See also **Appendix A – SLA, Appendix E – Escalation Contacts, Appendix F – Improvement Log**)*

- **Structured Severity Model:** Critical to Low incidents managed with clear response and resolution timelines.
- **Post-Incident Communication:** PIRs within 5 business days for High and Critical events, including root cause, remediation, and preventative measures.
- **Transparent Case Management:** All incidents logged in Freshdesk, integrated with Azure DevOps, visible to authorised Department stakeholders.
- **Continuous Learning:** Quarterly trend analysis to detect recurring issues, feeding into system and training improvements.

8. Business Continuity & Disaster Recovery Alignment

This section sets out CredEntry's approach to resilience, recovery, and continuity planning, ensuring compliance with Schedule 5 and WA Cyber Security Policy. It describes recovery objectives and planned annual testing with government stakeholders.

*(See also **Appendix G – BCP & DRP, Appendix H – Recovery Runbooks**)*

- **Resilience Strategy:** Multi-region Azure deployment, sovereign key management, and zero-trust access model.
- **Recovery Objectives:** Critical services restored within 2–4 hrs (RTO); data integrity protected to within 15–30 minutes (RPO).
- **Testing & Assurance:** Monthly backup restores, quarterly failover simulations, and annual scenario-based continuity exercises.
- **BCP Coverage:** Verification, revocation, issuance, SDK/API endpoints, and dashboard prioritised as critical services in the BCP impact matrix.

9. Governance, Reporting, and Reviews

This section defines governance processes, reporting obligations, and performance review mechanisms. It integrates SLA monitoring, compliance obligations (CR-1 to CR-5), and continuous improvement activities into one structured framework.

(See also Appendix D – Reporting Matrix, Appendix F – Improvement Log, Appendix I – Standards Mapping)

- **Governance Meetings:** Monthly contract management meetings to review KPIs, incidents, service levels, and planned improvements.
- **Formal Escalations:** Corrective Action Plans (CAPs) and Performance Remediation Plans (PRPs) delivered in line with Schedule 6 obligations.
- **Regular Reporting:** Monthly SLA compliance reports, quarterly trend analysis, annual performance review and roadmap discussion.

Enhanced Reporting Alignment (CR-1 to CR-5):

- Standards conformance results (ISO/IEC 18013, 23220, eIDAS 2.0).
- 24-hour cybersecurity incident reporting.
- Annual certification evidence (ISO/IEC 27001, SOC2, IRAP).
- Entity information security assurance.

10. Appendices

This section lists the supporting evidence pack that underpins the Support & Maintenance Framework.

Appendix E.1 – Service Level Agreement

Appendix E.2 – Training Plan

Appendix E.3 – Release & Onboarding Process Flow

Appendix E.4 – Reporting Matrix

Appendix E.5 – Communications Templates & Emergency Escalation Contacts

Appendix E.6 – Testing Results & Improvement Log

Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan

Appendix E.8 – Recovery Runbooks & Checklists

Appendix E.9 – Standards Compliance Mapping