

# CALMSHELL Master Policy Framework

## Implementation Roadmap

**Version:** 1.0

**Date:** June 2026

**Timeline:** 21 weeks (5 months)

---

## Executive Summary

This roadmap provides a structured approach to implementing the CALMSHELL Master Policy Framework across 21 weeks. The implementation is divided into three phases with specific milestones, deliverables, and success criteria.

---

## Phase 1 Implementation: Core Legal & Platform Policies

**Duration:** 4 weeks (Weeks 1-4)

**Policies:** 5

**Implementation Tasks:** 40+

### Week 1: Planning & Preparation

#### Monday-Tuesday: Kickoff & Team Assembly

- ☐ Conduct implementation kickoff meeting with all stakeholders
- ☐ Assign implementation team leads
- ☐ Review all Phase 1 policies
- ☐ Identify resource requirements
- ☐ Establish communication channels

#### Wednesday-Thursday: Legal Review

- ☐ Conduct legal review of Phase 1 policies
- ☐ Identify jurisdiction-specific requirements
- ☐ Prepare customization list

- ☐ Engage external counsel if needed

### **Friday: Planning & Scheduling**

- ☐ Create detailed implementation schedule
- ☐ Assign specific tasks to team members
- ☐ Set up project tracking system
- ☐ Schedule weekly status meetings

### **Deliverables:**

- Implementation plan document
  - Team assignments and responsibilities
  - Project tracking spreadsheet
  - Legal review notes
- 

## **Week 2: Policy Customization & Development**

### **Monday-Tuesday: Terms of Service**

- ☐ Customize Terms of Service with organizational details
- ☐ Add specific platform features and services
- ☐ Include payment terms and subscription details
- ☐ Review with legal counsel

### **Wednesday: Privacy Policy**

- ☐ Customize Privacy Policy with data practices
- ☐ Document all data collection points
- ☐ Specify third-party integrations
- ☐ Review with privacy officer

### **Thursday: Consent & Accessibility**

- ☐ Develop Consent to Services forms
- ☐ Create Accessibility Policy documentation
- ☐ Develop Cookie Policy implementation plan

### **Friday: Review & Approval**

- ☐ Executive review of all Phase 1 policies
- ☐ Obtain executive approval
- ☐ Prepare for implementation

**Deliverables:**

- Customized Terms of Service
  - Customized Privacy Policy
  - Consent forms and templates
  - Accessibility documentation
  - Executive approval documentation
- 

**Week 3: Platform Integration & Development****Monday-Tuesday: Website Integration**

- ☐ Integrate Terms of Service into website
- ☐ Integrate Privacy Policy into website
- ☐ Integrate Cookie Policy into website
- ☐ Create policy acceptance mechanism

**Wednesday-Thursday: Mobile App Integration**

- ☐ Integrate policies into mobile apps
- ☐ Create in-app policy acceptance
- ☐ Implement cookie consent banner
- ☐ Test on iOS and Android

**Friday: Testing & QA**

- ☐ Conduct comprehensive testing
- ☐ Verify all policies are accessible
- ☐ Test policy acceptance flow
- ☐ Fix any issues identified

**Deliverables:**

- Policies integrated into website
  - Policies integrated into mobile apps
  - Policy acceptance mechanism working
  - QA testing report
-

## **Week 4: Staff Training & Launch**

### **Monday-Tuesday: Staff Training**

- ☐ Conduct privacy training for all staff
- ☐ Conduct confidentiality training
- ☐ Conduct accessibility training
- ☐ Provide training materials and resources

### **Wednesday-Thursday: Support Preparation**

- ☐ Create FAQ about policies
- ☐ Train customer support team
- ☐ Create support documentation
- ☐ Prepare for user questions

### **Friday: Launch & Monitoring**

- ☐ Launch Phase 1 policies
- ☐ Monitor for issues
- ☐ Collect user feedback
- ☐ Make any necessary adjustments

### **Deliverables:**

- Staff training completion records
  - FAQ documentation
  - Support team training materials
  - Launch report and feedback summary
- 

## **Phase 2 Implementation: Clinical & Therapy Policies**

**Duration:** 6 weeks (Weeks 5-10)

**Policies:** 7

**Implementation Tasks:** 60+

## **Week 5: Clinical Policy Development**

### **Monday-Tuesday: Therapist Verification & Scope of Practice**

- ☐ Develop therapist application process
- ☐ Create credential verification procedures

- ☐ Establish regulatory body verification system
- ☐ Create therapist onboarding materials

### **Wednesday-Thursday: Telehealth & Crisis Response**

- ☐ Develop virtual care standards
- ☐ Create crisis response procedures
- ☐ Develop safety planning templates
- ☐ Establish 24/7 crisis hotline

### **Friday: Review & Approval**

- ☐ Clinical director review of all policies
- ☐ Obtain clinical approval
- ☐ Prepare for implementation

### **Deliverables:**

- Therapist verification procedures
  - Virtual care standards documentation
  - Crisis response procedures
  - Safety planning templates
- 

## **Week 6: Clinical Systems Development**

### **Monday-Tuesday: Documentation & AI Systems**

- ☐ Develop clinical documentation templates
- ☐ Create session note system
- ☐ Develop treatment plan templates
- ☐ Establish AI recommendation framework

### **Wednesday-Thursday: Postpartum Pathway**

- ☐ Develop postpartum screening tools
- ☐ Create postpartum assessment procedures
- ☐ Develop perinatal mental health resources
- ☐ Create infant safety assessment procedures

### **Friday: Integration Planning**

- ☐ Plan system integration
- ☐ Identify technology requirements

- ☐ Prepare implementation schedule

**Deliverables:**

- Clinical documentation system design
  - Postpartum pathway procedures
  - Screening and assessment tools
  - AI recommendation framework
- 

## **Week 7: Technology Implementation**

### **Monday-Tuesday: Therapist Verification System**

- ☐ Implement therapist application portal
- ☐ Integrate credential verification
- ☐ Implement license monitoring system
- ☐ Create therapist profile system

### **Wednesday-Thursday: Clinical Documentation System**

- ☐ Implement documentation templates
- ☐ Create session note system
- ☐ Implement treatment plan system
- ☐ Create progress note system

### **Friday: Testing & QA**

- ☐ Test therapist verification system
- ☐ Test clinical documentation system
- ☐ Conduct comprehensive QA
- ☐ Fix any issues identified

**Deliverables:**

- Therapist verification system operational
  - Clinical documentation system operational
  - QA testing report
  - System documentation
-

## **Week 8: Crisis Response & Virtual Care Implementation**

### **Monday-Tuesday: Crisis Response System**

- ☐ Implement crisis hotline system
- ☐ Create crisis escalation procedures
- ☐ Implement safety planning system
- ☐ Create crisis resource database

### **Wednesday-Thursday: Virtual Care Implementation**

- ☐ Implement video therapy platform
- ☐ Add real-time captioning
- ☐ Implement chat therapy system
- ☐ Create virtual care assessment tool

### **Friday: Testing & QA**

- ☐ Test crisis response system
- ☐ Test virtual care platform
- ☐ Conduct comprehensive QA
- ☐ Fix any issues identified

### **Deliverables:**

- Crisis response system operational
  - Virtual care platform operational
  - QA testing report
  - System documentation
- 

## **Week 9: Therapist Training & Onboarding**

### **Monday-Tuesday: Therapist Training Program**

- ☐ Develop therapist training materials
- ☐ Create clinical standards training
- ☐ Create crisis response training
- ☐ Create documentation training

### **Wednesday-Thursday: Therapist Onboarding**

- ☐ Begin therapist verification process
- ☐ Conduct therapist training

- ☐ Verify credentials and licenses
- ☐ Onboard initial therapist cohort

### **Friday: Monitoring & Support**

- ☐ Monitor therapist onboarding
- ☐ Provide support and guidance
- ☐ Collect feedback
- ☐ Make adjustments as needed

### **Deliverables:**

- Therapist training program complete
  - Initial therapists onboarded
  - Training completion records
  - Feedback and adjustment notes
- 

## **Week 10: Launch & Monitoring**

### **Monday-Tuesday: Soft Launch**

- ☐ Soft launch with limited therapist cohort
- ☐ Monitor system performance
- ☐ Collect feedback
- ☐ Make adjustments

### **Wednesday-Thursday: Full Launch**

- ☐ Expand to full therapist network
- ☐ Monitor for issues
- ☐ Provide support
- ☐ Collect user feedback

### **Friday: Post-Launch Review**

- ☐ Conduct post-launch review
- ☐ Document lessons learned
- ☐ Prepare Phase 3 implementation

### **Deliverables:**

- Phase 2 launch report
- System performance data

- User feedback summary
  - Lessons learned documentation
- 

## **Phase 3 Implementation: Health Information & Security Policies**

**Duration:** 5 weeks (Weeks 11-15)

**Policies:** 4

**Implementation Tasks:** 50+

### **Week 11: Security Infrastructure Planning**

#### **Monday-Tuesday: Data Protection Assessment**

- ☐ Conduct data classification audit
- ☐ Document all data types and sensitivity
- ☐ Review current encryption standards
- ☐ Identify gaps and requirements

#### **Wednesday-Thursday: Security Architecture**

- ☐ Design encryption architecture
- ☐ Design access control system
- ☐ Design audit logging system
- ☐ Design backup and recovery system

#### **Friday: Planning & Approval**

- ☐ CISO review of security architecture
- ☐ Obtain security approval
- ☐ Prepare implementation plan

#### **Deliverables:**

- Data classification audit report
  - Security architecture documentation
  - Implementation plan
  - Security approval documentation
-

## **Week 12: Encryption & Access Control Implementation**

### **Monday-Tuesday: Encryption Implementation**

- ☐ Implement TLS 1.2+ for all web traffic
- ☐ Implement certificate pinning in mobile apps
- ☐ Implement AES-256 encryption for databases
- ☐ Implement file system encryption

### **Wednesday-Thursday: Key Management & Access Control**

- ☐ Establish key management system
- ☐ Implement key rotation procedures
- ☐ Implement multi-factor authentication
- ☐ Implement role-based access control

### **Friday: Testing & Verification**

- ☐ Test encryption implementation
- ☐ Verify TLS configuration
- ☐ Test key rotation procedures
- ☐ Verify access control

### **Deliverables:**

- Encryption implementation complete
  - Key management system operational
  - Access control system operational
  - Testing report
- 

## **Week 13: Audit Logging & Monitoring Implementation**

### **Monday-Tuesday: Audit Logging System**

- ☐ Implement audit logging for all data access
- ☐ Create immutable log storage
- ☐ Implement log retention procedures
- ☐ Create log analysis tools

### **Wednesday-Thursday: Monitoring & Alerting**

- ☐ Implement intrusion detection system (IDS)
- ☐ Implement endpoint detection & response (EDR)

- ☐ Implement SIEM system
- ☐ Create alerting procedures

#### **Friday: Testing & Verification**

- ☐ Test audit logging system
- ☐ Test monitoring and alerting
- ☐ Verify log integrity
- ☐ Conduct comprehensive testing

#### **Deliverables:**

- Audit logging system operational
  - Monitoring and alerting operational
  - Testing report
  - System documentation
- 

### **Week 14: Backup, Recovery & Incident Response**

#### **Monday-Tuesday: Backup & Recovery System**

- ☐ Implement automated backup system
- ☐ Implement backup encryption
- ☐ Implement backup retention procedures
- ☐ Test backup recovery procedures

#### **Wednesday-Thursday: Incident Response System**

- ☐ Develop incident response procedures
- ☐ Create incident response team
- ☐ Implement incident classification system
- ☐ Create incident response templates

#### **Friday: Testing & Drills**

- ☐ Test backup recovery procedures
- ☐ Conduct incident response drill
- ☐ Test disaster recovery procedures
- ☐ Verify all systems operational

#### **Deliverables:**

- Backup and recovery system operational

- Incident response procedures documented
  - Incident response team established
  - Testing and drill reports
- 

## **Week 15: Staff Training & Launch**

### **Monday-Tuesday: IT Security Training**

- ☐ Conduct encryption training
- ☐ Conduct access control training
- ☐ Conduct incident response training
- ☐ Conduct data protection training

### **Wednesday-Thursday: All-Staff Training**

- ☐ Conduct confidentiality training
- ☐ Conduct data protection training
- ☐ Conduct security awareness training
- ☐ Provide training materials

### **Friday: Launch & Monitoring**

- ☐ Launch Phase 3 security measures
- ☐ Monitor for issues
- ☐ Provide support
- ☐ Collect feedback

### **Deliverables:**

- Staff training completion records
  - Training materials and resources
  - Launch report
  - Feedback summary
- 

## **Integration & Testing Phase**

**Duration:** 6 weeks (Weeks 16-21)

## **Week 16-17: Integration Testing**

### **Activities:**

- ☐ Test integration of all policies
- ☐ Verify all systems working together
- ☐ Conduct end-to-end testing
- ☐ Test user workflows
- ☐ Fix any integration issues

### **Deliverables:**

- Integration testing report
  - Issue resolution log
  - System documentation
- 

## **Week 18-19: Compliance Verification**

### **Activities:**

- ☐ Conduct compliance audit
- ☐ Verify PIPEDA compliance
- ☐ Verify PHIPA compliance
- ☐ Verify AODA compliance
- ☐ Document compliance evidence

### **Deliverables:**

- Compliance audit report
  - Compliance documentation
  - Regulatory evidence file
- 

## **Week 20-21: Final Review & Optimization**

### **Activities:**

- ☐ Conduct final review of all policies
- ☐ Gather feedback from all teams
- ☐ Identify optimization opportunities
- ☐ Document lessons learned

- ☐ Prepare for ongoing maintenance

**Deliverables:**

- Final review report
  - Optimization recommendations
  - Lessons learned documentation
  - Maintenance procedures
- 

## Resource Requirements

**Personnel****Executive Leadership (5% time)**

- CEO
- CISO
- CCO
- General Counsel

**Core Implementation Team (100% time)**

- Legal Counsel (2 FTE)
- Clinical Director (1 FTE)
- IT Security Manager (1 FTE)
- Compliance Manager (1 FTE)
- Project Manager (1 FTE)

**Supporting Teams (20-50% time)**

- IT Infrastructure Team (3-5 people)
- Development Team (3-5 people)
- HR Team (1-2 people)
- Support Team (1-2 people)
- QA Team (1-2 people)

**Total Resource Requirement:** 15-20 FTE equivalent

---

## Technology & Tools

**Required Systems:**

- Key management system (AWS KMS, HashiCorp Vault)
- Intrusion detection system (Snort, Suricata)
- Endpoint detection & response (CrowdStrike, Sentinel One)
- SIEM system (Splunk, ELK Stack)
- Vulnerability scanning tools (Nessus, Qualys)
- Penetration testing tools (Burp Suite, Metasploit)

**Estimated Technology Cost:** \$50,000-\$150,000

---

## Budget Estimate

| Category             | Cost                |
|----------------------|---------------------|
| Personnel (21 weeks) | \$300,000-\$500,000 |
| Technology & Tools   | \$50,000-\$150,000  |
| External Consulting  | \$50,000-\$100,000  |
| Training & Materials | \$20,000-\$50,000   |
| Total                | \$420,000-\$800,000 |

---

## Success Criteria

**Phase 1 Success Criteria**

- ☐ All 5 policies customized and approved
- ☐ Policies integrated into website and apps
- ☐ 100% staff training completion

- ☐ Zero critical issues at launch
- ☐ User acceptance > 95%

## Phase 2 Success Criteria

- ☐ All 7 policies implemented
- ☐ 50+ therapists onboarded
- ☐ Crisis response system operational
- ☐ Clinical documentation system operational
- ☐ Zero critical issues at launch

## Phase 3 Success Criteria

- ☐ All 4 policies implemented
- ☐ Encryption operational for all sensitive data
- ☐ Access control system operational
- ☐ Incident response team trained
- ☐ Disaster recovery tested and verified

## Overall Success Criteria

- ☐ All 16 policies implemented
  - ☐ 100% regulatory compliance
  - ☐ Zero critical security issues
  - ☐ 100% staff training completion
  - ☐ Positive user feedback
  - ☐ Ready for external audit
- 

## Risk Management

### High-Risk Items

#### Risk 1: Scope Creep

- **Mitigation:** Strict change control process, executive oversight
- **Owner:** Project Manager

#### Risk 2: Resource Constraints

- **Mitigation:** Early resource planning, contingency staffing
- **Owner:** HR Team

### **Risk 3: Technology Integration Issues**

- **Mitigation:** Early testing, vendor support, contingency plans
- **Owner:** IT Team

### **Risk 4: Regulatory Changes**

- **Mitigation:** Regular regulatory monitoring, policy flexibility
- **Owner:** Legal Team

### **Risk 5: Staff Resistance**

- **Mitigation:** Clear communication, training, change management
  - **Owner:** HR Team
- 

## **Communication Plan**

### **Stakeholder Updates**

- **Weekly:** Core implementation team meetings
- **Bi-weekly:** Executive steering committee meetings
- **Monthly:** All-staff updates
- **Quarterly:** Board updates

### **Communication Channels**

- Email updates
  - Team meetings
  - All-hands meetings
  - Intranet/internal wiki
  - Policy documentation
-

## Contingency Plans

### If Behind Schedule

- ☐ Prioritize critical policies
- ☐ Extend timeline if necessary
- ☐ Allocate additional resources
- ☐ Reduce scope if needed

### If Technology Issues Arise

- ☐ Engage vendor support immediately
- ☐ Identify workarounds
- ☐ Escalate to CISO
- ☐ Adjust timeline if needed

### If Regulatory Changes Occur

- ☐ Conduct impact assessment
  - ☐ Update affected policies
  - ☐ Communicate changes to team
  - ☐ Adjust implementation plan
- 

## Post-Implementation

### Ongoing Maintenance (After Week 21)

#### Monthly Activities:

- ☐ Review incident reports
- ☐ Monitor compliance metrics
- ☐ Update policy documentation
- ☐ Address user feedback

#### Quarterly Activities:

- ☐ Conduct compliance audit
- ☐ Review and update policies
- ☐ Conduct security testing

- ☐ Review incident response procedures

**Annual Activities:**

- ☐ Comprehensive compliance audit
  - ☐ Policy review and updates
  - ☐ Penetration testing
  - ☐ Disaster recovery testing
  - ☐ Staff training updates
- 

## Conclusion

This implementation roadmap provides a structured approach to implementing the CALMSHELL Master Policy Framework over 21 weeks. Success requires strong executive leadership, dedicated resources, and clear communication with all stakeholders.

**Key Success Factors:**

- 1 Executive commitment and oversight
  - 2 Dedicated implementation team
  - 3 Clear communication and change management
  - 4 Adequate resources and budget
  - 5 Regular monitoring and adjustment
- 

**Document Status:** Draft for Implementation

**Prepared By:** CALMSHELL Implementation Team

**Date:** June 2026

**Version:** 1.0