CALMSHELL PHASE 3: IMPLEMENTATION PROCEDURES & OPERATIONAL GUIDELINES

Complete Step-by-Step Procedures for All Policies

Canada / Ontario Edition — Version 1.0

EXECUTIVE OVERVIEW

Phase 3 provides detailed, step-by-step operational procedures for implementing all CALMSHELL policies established in Phases 1 and 2. This document is designed for operational staff, system administrators, and clinical teams responsible for day-to-day implementation of compliance procedures.

Document Structure:

- 10 operational procedure sections (one per major policy area)
- 50+ detailed step-by-step procedures
- 30+ operational checklists
- 20+ templates and forms
- Implementation timeline
- Staff role definitions
- System setup procedures

Target Audience: Operations managers, clinical supervisors, system administrators, compliance officers, and all CALMSHELL staff.

SECTION 1: TERMS OF SERVICE IMPLEMENTATION

1.1 User Onboarding Procedure

Objective: Ensure all new users acknowledge and accept Terms of Service before accessing platform.

Responsible Party: Onboarding Team / System Administrator

Step-by-Step Procedure:

Step 1: Pre-Registration (Before User Creates Account)

The system displays a clear notice: "By creating an account, you agree to our Terms of Service and Privacy Policy." This notice appears before the registration form.

Step 2: Registration Form Completion

User completes registration with required fields: email, password, full name, date of birth, and phone number. The system validates all fields and confirms password strength (minimum 12 characters, mixed case, numbers, symbols).

Step 3: Terms of Service Display

After registration, the system displays the complete Terms of Service in an easy-to-read format. The user must scroll through the entire document (system tracks scrolling to completion).

Step 4: Explicit Consent

User must check three mandatory boxes:

- "I have read and understand the Terms of Service"
- "I acknowledge that Calmshell is not a healthcare provider"
- "I understand emergency limitations and will contact 911 in emergencies"

Step 5: Signature & Timestamp

User provides electronic signature (typed name) and timestamp is automatically recorded. System generates unique consent record ID.

Step 6: Confirmation

System displays confirmation message: "Your account has been created and Terms of Service accepted. You can now access Calmshell."

Step 7: Documentation

System stores:

- Consent form with timestamp
- User IP address and device information
- Consent record ID
- Acceptance date and time

Step 8: Email Confirmation

Confirmation email sent to user with:

- Consent acceptance confirmation
- Copy of Terms of Service
- Link to Privacy Policy
- Support contact information

1.2 Terms of Service Modification Procedure

Objective: Implement changes to Terms of Service while maintaining user compliance.

Responsible Party: Legal Team / Compliance Officer

Procedure:

Step 1: Draft Changes

Legal team drafts proposed changes with clear explanation of what changed and why. Changes are reviewed by executive governance and clinical governance.

Step 2: Approval

Executive and clinical governance approve changes. Approval recorded in governance meeting minutes.

Step 3: Implementation Planning

Compliance team plans implementation including:

- Effective date (minimum 30 days notice)
- User notification strategy
- System updates required
- Staff training needed
- Transition procedures

Step 4: User Notification

Minimum 30 days before effective date, users receive notification via:

- Email with summary of changes
- In-app notification with link to full terms
- Website banner highlighting changes

- Support team briefing

Step 5: System Update

System is updated with new Terms of Service. Old version is archived with effective date.

Step 6: Re-Consent Process

Users must re-accept new Terms of Service before continuing to use platform. System tracks re-consent with new timestamp and consent record ID.

Step 7: Documentation

All changes, approvals, notifications, and re-consent records are documented and stored.

Step 8: Verification

Compliance team verifies that 100% of active users have accepted new terms before enforcement date.

1.3 Terms of Service Violation Response Procedure

Objective: Respond appropriately to user violations of Terms of Service.

Responsible Party: Community Moderation Team / Compliance Officer

Procedure:

Step 1: Violation Detection

Violation is detected through:

- User report
- Automated system monitoring
- Staff observation
- Community moderation review

Step 2: Documentation

Violation is documented with:

- Date and time of violation
- Description of violation
- Evidence (screenshots, posts, messages)

- Reporter name and contact
- Violation category (prohibited use)

Step 3: Initial Review

Moderation team reviews documentation to confirm violation. If unclear, additional investigation is conducted.

Step 4: Severity Assessment

Violation is classified as:

- Minor (warning level)
- Moderate (suspension level)
- Severe (termination level)

Step 5: User Notification

User is notified of violation with:

- Clear explanation of what violated terms
- Evidence of violation
- Consequences (warning, suspension, or termination)
- Appeal process and timeline
- Support contact information

Step 6: Action Implementation

Based on severity:

- **Minor:** Warning issued, documented in user file
- **Moderate:** Account suspended for specified period (7-30 days), user notified
- **Severe:** Account terminated, user notified with appeal information

Step 7: Appeal Process

User has 14 days to appeal decision. Appeal is reviewed by independent compliance officer. Decision is final.

Step 8: Documentation

All actions, notifications, and appeals are documented in user compliance file.

SECTION 2: PRIVACY POLICY IMPLEMENTATION

2.1 Data Collection Procedure

Objective: Collect only necessary personal and health information with proper consent.

Responsible Party: Data Collection Team / System Administrator

Procedure:

Step 1: Determine Data Needs

For each data collection point, determine:

- What data is necessary
- Why it is necessary
- How it will be used
- How long it will be retained
- Who will have access

Step 2: Minimize Data Collection

Collect only data that is necessary. Do not collect "nice to have" data. Apply data minimization principle.

Step 3: Obtain Consent

Before collecting data, obtain explicit user consent through:

- Clear notice of what data is being collected
- Explanation of why it is being collected
- Explanation of how it will be used
- Opportunity to decline (if not essential)

Step 4: Collect Data

Data is collected through:

- User input (registration forms, profiles)
- System tracking (usage analytics, device information)
- Third-party sources (with consent)
- Therapist input (with user consent)

Step 5: Verify Accuracy

Data accuracy is verified through:

- User review and confirmation
- System validation rules
- Periodic user verification

Step 6: Secure Storage

Data is stored securely with:

- Encryption at rest (AES-256)
- Encryption in transit (HTTPS)
- Access controls (role-based)
- Audit logging

Step 7: Document Collection

All data collection is documented with:

- Date and time of collection
- Consent record ID
- Data type and purpose
- User acknowledgment

2.2 Privacy Rights Request Procedure

Objective: Respond to user requests for access, correction, or deletion of personal information.

Responsible Party: Privacy Officer / Data Management Team

Procedure:

Step 1: Receive Request

User submits privacy rights request through:

- Online request form
- Email to privacy officer
- Phone call to privacy office
- In-person request

Request must include:

- User name and account ID
- Type of request (access, correction, deletion, accounting)
- Specific information requested (if applicable)
- Contact information for response

Step 2: Verify Identity

Privacy officer verifies user identity through:

- Account verification (email and password)
- Security questions
- Photo ID verification (if in-person)

Step 3: Assess Request

Request is assessed for:

- Validity (is it a legitimate privacy right)
- Scope (what information is requested)
- Complexity (simple or complex)
- Legal obligations (retention requirements)

Step 4: Determine Response Timeline

Response timeline is determined based on request type:

- Access request: 30 days
- Correction request: 30 days
- Deletion request: 30 days (subject to retention)
- Accounting of disclosures: 30 days

Step 5: Prepare Response

Response is prepared including:

- Requested information in clear format
- Explanation of any information withheld (with reason)
- Information about retention or deletion
- Next steps and appeal process

Step 6: Deliver Response

Response is delivered to user through:

- Secure email
- Secure portal download
- In-person meeting
- Certified mail

Step 7: Document Request

All privacy requests are documented with:

- Request date and type
- User identification
- Response date and content
- Any appeals or follow-up

Step 8: Follow-Up

User is contacted to confirm satisfaction with response. If user is not satisfied, appeal process is explained.

2.3 Data Breach Response Procedure

Objective: Respond quickly and appropriately to any data breach or security incident.

Responsible Party: Security Team / Privacy Officer / Executive Leadership

Procedure:

Step 1: Detect Breach

Breach is detected through:

- Automated monitoring systems
- User report
- Staff notification
- Security audit findings

Step 2: Immediate Containment

Upon detection:

- Isolate affected systems
- Stop unauthorized access
- Preserve evidence
- Notify security team

Step 3: Assess Breach

Breach is assessed for:

- Type of data compromised
- Number of individuals affected
- Severity of risk to individuals
- Likely cause of breach

- Scope of compromise

Step 4: Notify Leadership

Executive leadership is notified immediately with:

- Breach description
- Data compromised
- Individuals affected
- Severity assessment
- Recommended actions

Step 5: Investigate Breach

Investigation is conducted to determine:

- How breach occurred
- When it occurred
- What data was accessed
- Whether data was copied or deleted
- Whether breach is ongoing

Step 6: Notify Affected Individuals

If breach poses risk to individuals, affected individuals are notified within 30 days with:

- Description of breach
- Data compromised
- Steps they should take
- Support resources available
- Contact information for questions

Step 7: Notify Regulators

If breach meets notification threshold, regulators are notified:

- Privacy Commissioner of Ontario (if Ontario residents affected)
- Other regulators as required
- Notification includes breach details and response plan

Step 8: Remediation

Steps are taken to:

- Fix the vulnerability
- Prevent future breaches
- Restore affected systems

- Improve security procedures

Step 9: Documentation

Complete breach documentation is maintained including:

- Breach report
- Investigation findings
- Notifications sent
- Remediation actions
- Lessons learned

Step 10: Review & Improvement

Breach is reviewed to identify:

- Root cause
- Systemic issues
- Improvements needed
- Policy updates required

SECTION 3: CONSENT MANAGEMENT IMPLEMENTATION

3.1 Consent Form Administration Procedure

Objective: Ensure all consent forms are properly completed, documented, and stored.

Responsible Party: Clinical Staff / Consent Coordinator

Procedure:

Step 1: Identify Consent Need

For each user interaction, determine what consent is needed:

- Platform consent (all users)
- Wellness tool consent (wellness users)
- Therapy consent (therapy users)
- Specialized program consent (program participants)

Step 2: Prepare Consent Form

Appropriate consent form is prepared including:

- Clear explanation of what is being consented to
- Risks and benefits
- Alternatives
- Right to withdraw consent
- Contact information for questions

Step 3: Present to User

Consent form is presented to user through:

- Digital form (for online users)
- Printed form (for in-person users)
- Verbal explanation (supplementing written form)

Step 4: Answer Questions

User is given opportunity to ask questions. All questions are answered clearly and documented.

Step 5: Obtain Signature

User provides signature (electronic or handwritten) confirming understanding and agreement. Timestamp is recorded.

Step 6: Provide Copy

User is provided with copy of signed consent form through:

- Email (digital copy)
- Printed copy (in-person)
- Portal download (online)

Step 7: Store Original

Original signed consent form is stored securely with:

- User file
- Secure storage location
- Access controls
- Backup copy

Step 8: Document in System

Consent is documented in system with:

- Consent type
- Date and time
- User signature
- Witness (if applicable)
- Consent record ID

3.2 Consent Withdrawal Procedure

Objective: Allow users to withdraw consent while maintaining appropriate records.

Responsible Party: Clinical Staff / Compliance Officer

Procedure:

Step 1: Receive Withdrawal Request

User requests to withdraw consent through:

- Online form
- Email
- Phone call
- In-person meeting

Step 2: Clarify Request

Staff clarifies what consent is being withdrawn and what implications this has:

- Therapy services will end
- Wellness tools will be unavailable
- Account may be closed
- Data will be handled per retention policy

Step 3: Document Request

Withdrawal request is documented with:

- Date and time
- Type of consent being withdrawn
- User acknowledgment of implications
- User signature

Step 4: Confirm Understanding

User confirms understanding of implications and confirms withdrawal request.

Step 5: Process Withdrawal

Upon confirmation:

- Services are stopped
- Account access is modified
- Data handling is updated per policy
- User is notified

Step 6: Store Documentation

Withdrawal request is stored with:

- Original consent form
- Withdrawal request
- Date of withdrawal
- Implications explained

Step 7: Follow-Up

User is contacted after withdrawal to:

- Confirm withdrawal was processed
- Offer support resources
- Provide information about re-engaging

SECTION 4: THERAPIST VERIFICATION & CREDENTIALING

4.1 Therapist Application & Credentialing Procedure

Objective: Verify that all therapists meet professional standards and are properly credentialed.

Responsible Party: Clinical Governance Team / Credentialing Coordinator

Procedure:

Step 1: Application Submission

Prospective therapist submits application including:

- Completed application form
- Curriculum vitae or professional summary
- Proof of active professional registration
- Professional liability insurance certificate
- References from colleagues or supervisors
- Signed agreement to Calmshell standards
- Photo identification
- Background authorization form

Step 2: Application Review

Application is reviewed for completeness. If incomplete, applicant is contacted to provide missing information.

Step 3: Credential Verification

Credentials are verified by contacting:

- Professional regulatory college (College of Psychologists of Ontario, College of Nurses of Ontario, etc.)
- Professional liability insurance provider
- References provided by applicant
- Previous employers (if applicable)

Verification confirms:

- Active professional registration
- No disciplinary history
- Professional liability insurance is current
- Scope of practice aligns with Calmshell services

Step 4: Background Check

Background check is conducted (if applicable based on role):

- Criminal record check
- Vulnerable sector check (if working with vulnerable populations)
- Reference checks

Step 5: Clinical Governance Review

Clinical governance reviews application and credentials to determine:

- Qualifications meet Calmshell standards
- Scope of practice is appropriate
- No conflicts of interest

- Recommendation for approval or denial

Step 6: Approval Decision

Clinical governance makes final approval decision:

- Approved (therapist can proceed to onboarding)
- Approved with conditions (specific requirements must be met)
- Denied (application is rejected with explanation)

Step 7: Notification

Applicant is notified of decision with:

- Clear statement of approval/denial
- If approved: onboarding timeline and next steps
- If denied: explanation of decision and appeal process

Step 8: Onboarding (If Approved)

Upon approval, therapist completes onboarding including:

- Calmshell orientation and training
- Platform technical training
- Privacy and confidentiality training
- Crisis response procedures
- Community guidelines training
- Initial supervision assignment

Step 9: Documentation

All credentialing documentation is stored with:

- Application and supporting documents
- Verification records
- Background check results
- Approval decision
- Onboarding completion

Step 10: Ongoing Compliance

Therapist compliance is monitored through:

- Annual credential renewal verification
- Supervision records
- Performance reviews
- Complaint tracking

- Continuing education documentation

4.2 Therapist Supervision Procedure

Objective: Ensure therapists receive appropriate supervision and maintain clinical standards.

Responsible Party: Clinical Supervisor / Clinical Governance

Procedure:

Step 1: Assign Supervisor

Upon therapist approval, supervisor is assigned based on:

- Therapist's discipline and experience
- Supervisor's expertise and availability
- Clinical governance recommendation

Step 2: Schedule Supervision

Supervision schedule is established:

- New therapists: Weekly supervision (first 3 months)
- Established therapists: Monthly supervision minimum
- Specialized programs: Additional supervision as needed
- Crisis cases: Immediate supervision available

Step 3: Prepare for Supervision

Therapist prepares for supervision by:

- Selecting cases for discussion
- Preparing case summaries
- Identifying clinical questions or concerns
- Gathering relevant documentation

Step 4: Conduct Supervision

Supervision session includes:

- Case review and clinical discussion
- Feedback on clinical approach
- Identification of learning needs
- Discussion of challenges or concerns
- Planning for next cases

Step 5: Document Supervision

Supervision is documented with:

- Date and time
- Cases discussed
- Key learning points
- Recommendations
- Supervisor signature
- Therapist acknowledgment

Step 6: Follow-Up

Therapist implements recommendations from supervision:

- Adjusts clinical approach as needed
- Addresses identified learning needs
- Follows up on recommendations

Step 7: Escalation

If clinical concerns are identified:

- Immediate escalation to clinical governance
- Additional supervision may be required
- Performance improvement plan may be implemented
- Therapist may be suspended pending review

Step 8: Ongoing Monitoring

Supervision records are monitored to:

- Ensure supervision is occurring regularly
- Identify patterns or concerns
- Track therapist development
- Plan for continuing education

SECTION 5: CRISIS RESPONSE IMPLEMENTATION

5.1 Crisis Identification & Response Procedure

Objective: Quickly identify and appropriately respond to crisis situations.

Responsible Party: Therapist / Crisis Response Team / Clinical Governance

Procedure:

Step 1: Crisis Identification

Crisis is identified through:

- User self-report during therapy
- Therapist observation during session
- User message to support team
- Community post indicating crisis
- Automated alert system

Step 2: Initial Assessment

Upon identification, initial assessment is conducted to determine:

- Type of crisis (suicidal, homicidal, psychotic, substance, abuse, etc.)
- Severity and immediacy of risk
- Protective factors present
- Current location and access to means
- Support system availability

Step 3: Provide Immediate Support

Therapist or crisis responder:

- Listens without judgment
- Validates feelings and experiences
- Expresses care and concern
- Provides hope and support
- Avoids minimizing or dismissing

Step 4: Safety Assessment

Detailed safety assessment is conducted:

- Suicidal/homicidal ideation: Is there a plan? Access to means? Intent?
- Substance use: What substance? How much? When? Any overdose risk?
- Abuse: Is user in immediate danger? Is there a safe place to go?
- Psychosis: Is user at risk of harm due to delusions or hallucinations?

Step 5: Determine Response Level

Based on assessment, response is determined:

Level 1 - Imminent Danger (Immediate 911 Response):

- Active suicidal/homicidal intent with plan and means
- Acute psychosis with command hallucinations to harm
- Overdose or severe substance intoxication
- Active abuse with immediate danger

Response: Contact 911 immediately, provide location, stay with user if possible

Level 2 - High Risk (Urgent Professional Response):

- Suicidal ideation with some planning
- Severe depression or anxiety
- Substance use concerns
- Abuse concerns but not immediate danger

Response: Immediate crisis counseling, safety planning, referral to emergency services or crisis team

Level 3 - Moderate Risk (Enhanced Support):

- Suicidal thoughts but no plan
- Significant distress but coping
- Recent loss or trauma
- Substance use but stable

Response: Increased therapy frequency, safety planning, support resources, follow-up within 24 hours

Step 6: Implement Response

Response is implemented according to level:

- Level 1: Call 911, provide information, document incident
- Level 2: Immediate crisis counseling, safety planning, referral
- Level 3: Enhanced support, safety planning, follow-up scheduling

Step 7: Provide Resources

User is provided with crisis resources:

- National Suicide Prevention Lifeline: 1-833-456-4566
- Crisis Text Line: Text HOME to 741741
- Local crisis teams and hotlines
- Emergency department information
- Support group information

Step 8: Safety Planning

If appropriate, safety plan is developed with user including:

- Warning signs that crisis may be worsening
- Internal coping strategies
- People and social settings that provide distraction
- People to ask for help
- Professional resources and crisis lines
- Ways to make environment safer

Step 9: Documentation

Crisis incident is thoroughly documented with:

- Date and time of crisis
- Type of crisis
- Assessment findings
- Response taken
- Resources provided
- Follow-up plan
- Therapist/responder signature

Step 10: Follow-Up

User is contacted within 24 hours to:

- Check on safety and wellbeing
- Assess effectiveness of response
- Adjust safety plan if needed
- Schedule follow-up therapy
- Provide additional support

Step 11: Incident Review

Crisis incident is reviewed by clinical governance to:

- Assess appropriateness of response
- Identify any system improvements needed
- Provide support to therapist/responder
- Update procedures if needed

SECTION 6: BILLING & SUBSCRIPTION IMPLEMENTATION

6.1 Subscription Activation Procedure

Objective: Activate subscriptions securely and accurately.

Responsible Party: Billing Team / System Administrator

Procedure:

Step 1: User Selects Plan

User selects subscription plan from pricing page:

- Free plan
- Basic plan ($9.99/month or $99.90/year)
- Pro plan ($19.99/month or $199.90/year)
- Premium plan ($49.99/month or $499.90/year)

Step 2: Review Plan Details

System displays plan details including:

- Price and billing cycle
- Features included
- Cancellation policy
- Renewal information

Step 3: Provide Payment Information

User provides payment information:

- Credit card number, expiration, CVV
- Billing address
- Cardholder name

Step 4: Payment Processing

Payment is processed through Stripe:

- Card is validated
- Payment is authorized
- Transaction ID is generated
- Payment confirmation is received

Step 5: Subscription Activation

Upon successful payment:

- Subscription is activated in system
- Billing cycle begins
- User account is upgraded to selected plan
- Features are enabled

Step 6: Confirmation Email

Confirmation email is sent to user with:

- Subscription confirmation
- Plan details and price
- Billing cycle information
- Renewal date
- Cancellation instructions
- Support contact information

Step 7: Access Granted

User is granted access to plan features:

- Wellness tools (all plans)
- Community access (all plans)
- Therapy sessions (Pro and Premium)
- Premium features (Premium plan)

Step 8: Documentation

Subscription is documented with:

- Subscription ID
- User account ID
- Plan selected
- Activation date
- Billing cycle
- Payment method (last 4 digits only)
- Amount charged

6.2 Subscription Renewal Procedure

Objective: Automatically renew subscriptions while providing user control.

Responsible Party: Billing System / Billing Team

Procedure:

Step 1: Renewal Reminder

7 days before renewal date, user receives reminder email with:

- Renewal date
- Amount to be charged
- Plan details
- Cancellation instructions
- Confirmation that renewal will occur

Step 2: Automatic Payment Processing

On renewal date, payment is automatically processed:

- Stripe processes payment using stored card
- Transaction ID is generated
- Payment confirmation is received

Step 3: Payment Success

If payment is successful:

- Subscription is renewed for another billing cycle
- Confirmation email is sent to user
- Account access continues uninterrupted
- New renewal date is set

Step 4: Payment Failure

If payment fails:

- User is notified of payment failure
- Reason for failure is explained
- User is given 3 days to update payment method
- If not updated, subscription is suspended
- User is notified of suspension

Step 5: Subscription Suspension

If payment is not received:

- Subscription is suspended
- User account is downgraded to free plan
- Paid features are disabled

- User is notified of suspension

Step 6: Reactivation

User can reactivate subscription by:

- Updating payment method
- Reselecting subscription plan
- Confirming renewal

Step 7: Documentation

Renewal is documented with:

- Renewal date
- Amount charged
- Payment method
- Transaction ID
- Renewal confirmation

6.3 Subscription Cancellation Procedure

Objective: Allow users to cancel subscriptions easily while protecting their data.

Responsible Party: Billing Team / Customer Support

Procedure:

Step 1: Cancellation Request

User requests cancellation through:

- Account settings (self-service)
- Email to support
- Phone call to support
- In-person request

Step 2: Cancellation Confirmation

User is asked to confirm cancellation and is informed:

- Cancellation will take effect at end of billing cycle
- Access to paid features will end at that time
- Data will be retained per privacy policy
- Refund policy (if applicable)

Step 3: Refund Eligibility Check

System checks refund eligibility:

- If within 7 days of purchase: Full refund eligible
- If beyond 7 days: No refund (except prorated first month)
- If institutional plan: Custom refund terms apply

Step 4: Process Cancellation

Cancellation is processed:

- Subscription is marked for cancellation
- Cancellation date is set to end of billing cycle
- Recurring billing is stopped
- User is notified

Step 5: Refund Processing (If Eligible)

If refund is eligible:

- Refund amount is calculated
- Refund is processed through Stripe
- Refund confirmation is sent to user
- Refund appears in user's account within 2-5 business days

Step 6: Account Transition

At cancellation date:

- Subscription is deactivated
- User account is downgraded to free plan
- Paid features are disabled
- User data is retained
- User is notified

Step 7: Retention Outreach

User may receive outreach to:

- Understand reason for cancellation
- Offer alternative plans
- Provide special offers or discounts
- Maintain relationship

Step 8: Documentation

Cancellation is documented with:

- Cancellation date
- Reason for cancellation (if provided)
- Refund amount (if applicable)
- Refund date
- Account status change

SECTION 7: COMMUNITY MODERATION IMPLEMENTATION

7.1 Community Moderation Procedure

Objective: Maintain safe, respectful community while protecting user expression.

Responsible Party: Community Moderation Team

Procedure:

Step 1: Content Monitoring

Community content is monitored through:

- Automated keyword filtering
- User reports
- Staff review of community posts
- Regular audits of community activity

Step 2: Violation Detection

Potentially violating content is identified and flagged for review.

Step 3: Content Review

Flagged content is reviewed by moderator to determine:

- Is content actually a violation?
- What is the severity of violation?
- What is the appropriate response?

Step 4: Violation Classification

Violation is classified as:

- **Minor:** First-time violation, low severity (warning)
- **Moderate:** Repeated violation or moderate severity (content removal, temporary suspension)
- **Severe:** Serious violation, safety concern, hate speech (permanent removal, account suspension)

Step 5: Action Implementation

Based on classification:

Minor Violation:

- Warning message sent to user
- Content may be flagged or hidden
- User is educated about community guidelines
- Incident is documented

Moderate Violation:

- Content is removed from community
- User is notified of removal and reason
- User account may be suspended for 7-30 days
- User is given opportunity to appeal
- Incident is documented

Severe Violation:

- Content is immediately removed
- User account is suspended or terminated
- User is notified of action and reason
- Incident is escalated to clinical governance if safety concern
- Law enforcement may be contacted if illegal activity
- Incident is thoroughly documented

Step 6: User Notification

User is notified of action with:

- Clear explanation of what violated guidelines
- Evidence of violation (if appropriate)
- Action taken
- Appeal process and timeline
- Support resources

Step 7: Appeal Process

User can appeal moderation decision within 14 days by:

- Submitting appeal form
- Explaining why decision was wrong
- Providing additional context

Appeal is reviewed by independent moderator who was not involved in original decision. Decision is final.

Step 8: Documentation

All moderation actions are documented with:

- Date and time
- Content that violated
- Violation category
- Action taken
- User notification
- Appeal (if any)
- Final outcome

Step 9: Pattern Analysis

Moderation team regularly analyzes patterns to:

- Identify repeat violators
- Identify gaps in guidelines
- Identify training needs
- Improve moderation procedures

SECTION 8: INSTITUTIONAL DATA ACCESS IMPLEMENTATION

8.1 Educational Institution Data Access Procedure

Objective: Provide educational institutions with appropriate aggregate data while protecting individual privacy.

Responsible Party: Data Management Team / Privacy Officer

Procedure:

Step 1: Partnership Agreement

Educational institution enters into data access agreement including:

- Permitted data access
- Prohibited data access
- Data use restrictions
- Confidentiality obligations
- Audit rights
- Term and termination

Step 2: Data Access Request

Institution submits data access request specifying:

- Data requested
- Purpose of request
- Time period
- Frequency of access
- Intended use

Step 3: Request Review

Privacy officer reviews request to determine:

- Is data permitted under agreement?
- Is request for legitimate purpose?
- Are privacy protections adequate?
- Is data aggregated appropriately?

Step 4: Data Aggregation

Data is aggregated to protect privacy:

- Minimum 5 individuals per data point
- No identifiable information included
- Aggregate reporting only
- Trends and patterns only

Step 5: Data Delivery

Aggregated data is delivered through:

- Secure portal
- Encrypted email
- Secure file transfer

- In-person meeting

Step 6: Access Logging

All data access is logged with:

- Institution name
- Date and time of access
- Data accessed
- Purpose of access
- User who accessed data

Step 7: Compliance Monitoring

Ongoing monitoring ensures:

- Data is used only for permitted purposes
- Data is kept confidential
- Data is not re-identified
- Agreement terms are followed

Step 8: Annual Audit

Annual audit is conducted to:

- Verify data use compliance
- Confirm data security
- Review any incidents or concerns
- Renew or modify agreement

SECTION 9: CRISIS RESPONSE TEAM PROCEDURES

9.1 Crisis Response Team Roles & Responsibilities

Crisis Response Team Composition:

Role	Responsibility	Availability	Training
Crisis Coordinator	Oversee crisis response, escalate as needed	During business hours	Crisis intervention, mental health first aid

Role	Responsibility	Availability	Training
On-Call Therapist	Provide immediate crisis counseling	24/7 rotation	Crisis intervention, suicide risk assessment
Clinical Supervisor	Review crisis responses, provide guidance	During business hours	Crisis management, clinical supervision
Security Team	Respond to safety threats, contact authorities	24/7	Security procedures, threat assessment
Support Staff	Document incidents, follow up with users	During business hours	Incident documentation, support procedures

Crisis Response Escalation:

```
User in Crisis
    ↓
Therapist/Staff Identifies Crisis
    ↓
Initial Assessment (Severity Level 1, 2, or 3)
    ↓
Level 1: Call 911 Immediately → Notify Clinical Supervisor → Document
Level 2: Crisis Counseling → Safety Planning → Referral → Follow-up
Level 3: Enhanced Support → Safety Plan → Follow-up within 24 hours
    ↓
Clinical Governance Review
    ↓
Incident Documentation & Improvement
```

SECTION 10: STAFF TRAINING & COMPLIANCE

10.1 Staff Training Requirements

All Staff Training:

- Orientation (before first day)
- Privacy and confidentiality (annual)
- Crisis response (annual)
- Community guidelines (annual)
- Role-specific training (as needed)

Clinical Staff Training:

- All staff training (above)
- Clinical assessment and diagnosis (annual)
- Therapeutic techniques (annual)
- Supervision procedures (annual)
- Scope of practice (annual)

Administrative Staff Training:

- All staff training (above)
- Data management procedures (annual)
- Billing and subscription procedures (annual)
- Community moderation (annual)
- Customer support procedures (annual)

10.2 Staff Compliance Monitoring

Monitoring Procedures:

- Monthly compliance check-ins with supervisors
- Quarterly compliance audits
- Annual compliance certification
- Incident investigation and follow-up
- Performance reviews with compliance component

Compliance Metrics:

- Percentage of staff completing required training
- Incident response time
- Crisis response appropriateness
- User satisfaction with support
- Complaint resolution time

IMPLEMENTATION TIMELINE

Month 1: Foundation

- Staff training on all procedures
- System setup and testing
- Documentation templates preparation

- Initial policy rollout

Month 2: Operational Launch

- Begin implementing all procedures
- Monitor compliance
- Gather feedback
- Make adjustments

Month 3: Optimization

- Refine procedures based on feedback
- Improve efficiency
- Expand to all areas
- Prepare for audit

Months 4-6: Scaling

- Expand procedures to all operations
- Increase monitoring and auditing
- Develop specialized procedures
- Prepare for external audit

CONCLUSION

Phase 3 Implementation Procedures provide detailed, step-by-step guidance for implementing all CALMSHELL policies. These procedures ensure consistent, compliant operations across all areas of the platform.

Key Success Factors:

- Clear procedures that staff understand
- Adequate training and support
- Regular monitoring and feedback
- Continuous improvement
- Strong leadership and accountability

Document Version: 1.0
Status: Production-Ready
Last Updated: June 2026