CALMSHELL Master Policy Framework

Phase 3: Health Information & Security Policies

Document Version: 1.0
Effective Date: June 2026
Jurisdiction: Canada (Primary: Ontario, PIPEDA, PHIPA, Federal Regulations)
Last Updated: June 2026
Status: DRAFT FOR IMPLEMENTATION

Table of Contents

POLICY 13: DATA PROTECTION & ENCRYPTION POLICY

13.1 Purpose & Scope

The Data Protection & Encryption Policy establishes comprehensive standards for protecting personal information and health information collected by CALMSHELL. This policy ensures that data is encrypted, securely stored, backed up, and protected from unauthorized access, loss, or theft. The policy complies with PIPEDA, PHIPA, and industry-standard data protection practices.

CALMSHELL recognizes that users entrust sensitive personal and health information to the platform. Data protection is fundamental to maintaining user trust and complying with legal obligations.

13.2 Data Classification

CALMSHELL classifies data into categories based on sensitivity and regulatory requirements:

Tier 1 - Highly Sensitive Health Information:

- Mental health diagnoses and treatment information
- Therapy session notes and clinical records
- Suicide risk assessments and safety plans
- Medication information and psychiatric history
- Trauma history and sensitive personal disclosures
- Assessment responses and screening results
- Video/audio recordings of therapy sessions

Tier 2 - Sensitive Personal Information:

- Account credentials (passwords, authentication tokens)
- Payment information (credit card numbers, banking details)
- Government-issued identification numbers
- Contact information (phone, email, address)
- Emergency contact information
- Demographic information (age, gender, sexual orientation)

Tier 3 - General Information:

- Platform usage data and analytics
- De-identified research data
- Public profile information
- General engagement metrics

13.3 Encryption Standards

Encryption in Transit:

All data transmitted between user devices and CALMSHELL servers is encrypted using TLS 1.2 or higher. CALMSHELL implements:

- **HTTPS/TLS:** All web traffic uses HTTPS with TLS 1.2 or higher encryption
- **Certificate Management:** Valid SSL/TLS certificates from trusted certificate authorities
- **Certificate Pinning:** Mobile applications use certificate pinning to prevent man-in-the-middle attacks
- **Perfect Forward Secrecy:** Ephemeral key exchange to ensure session keys cannot be compromised if long-term keys are compromised

Video therapy sessions use end-to-end encryption with SRTP (Secure Real-time Transport Protocol) or equivalent encryption standards.

Encryption at Rest:

All data stored on CALMSHELL servers is encrypted using AES-256 encryption or equivalent. CALMSHELL implements:

- **Database Encryption:** All databases containing personal or health information are encrypted using AES-256
- **File System Encryption:** File systems containing sensitive data are encrypted using LUKS, BitLocker, or equivalent
- **Backup Encryption:** All backups are encrypted using AES-256 or equivalent
- **Key Management:** Encryption keys are managed securely and rotated regularly (at least annually)

Encryption Key Management:

- **Key Generation:** Encryption keys are generated using cryptographically secure random number generators
- **Key Storage:** Keys are stored in secure key management systems (e.g., AWS KMS, HashiCorp Vault) with restricted access
- **Key Rotation:** Keys are rotated annually or more frequently if compromise is suspected
- **Key Backup:** Keys are backed up securely and tested for recovery
- **Access Control:** Access to keys is restricted to authorized personnel and systems

13.4 Data Storage & Infrastructure

Storage Location:

All user data is stored on secure servers located in Canada, primarily in Ontario and other Canadian provinces. Data is not transferred outside Canada except:

- For service delivery by Canadian service providers (e.g., cloud hosting in Canada)
- With explicit user consent
- As required by law

CALMSHELL uses Canadian cloud providers (e.g., Amazon Web Services Canada, Microsoft Azure Canada) to ensure data residency compliance.

Infrastructure Security:

- **Physical Security:** Data centers are physically secured with access controls, surveillance, and environmental monitoring

- **Network Security:** Firewalls, intrusion detection systems, and network segmentation protect against unauthorized access
- **Server Hardening:** Servers are hardened with security updates, minimal services, and security configurations
- **Vulnerability Management:** Regular vulnerability scans and penetration testing identify and address security weaknesses

13.5 Access Control

Authentication:

- **Multi-Factor Authentication (MFA):** All staff accessing sensitive data use MFA (e.g., authenticator apps, hardware keys)
- **Strong Passwords:** Passwords must meet complexity requirements (minimum 12 characters, mixed case, numbers, symbols)
- **Password Management:** Passwords are managed securely using password managers
- **Session Management:** Sessions expire after 30 minutes of inactivity; users must re-authenticate for sensitive operations

Authorization:

- **Role-Based Access Control (RBAC):** Access to data is based on job role and need-to-know
- **Principle of Least Privilege:** Users are granted minimum access necessary to perform their functions
- **Segregation of Duties:** Sensitive functions (e.g., data deletion, access grants) require multiple approvals
- **Access Reviews:** Access is reviewed quarterly and revoked when no longer needed

Access Levels:

- **Tier 1 Data:** Access restricted to treating therapist, clinical supervisors, and authorized security/compliance staff
- **Tier 2 Data:** Access restricted to relevant staff (e.g., payment processors for payment data)
- **Tier 3 Data:** Access available to analytics and product teams for improvement purposes

13.6 Audit Logging & Monitoring

Access Logging:

All access to sensitive data is logged, including:

- User identity and authentication method

- Date, time, and duration of access
- Data accessed and actions performed
- IP address and device information
- Reason for access (if applicable)

Logs are retained for 2 years and are immutable (cannot be modified or deleted).

Monitoring & Alerting:

- **Real-Time Monitoring:** Automated systems monitor for suspicious access patterns (e.g., access outside normal hours, unusual data volumes)
- **Alerting:** Alerts are triggered for suspicious activities and investigated immediately
- **Anomaly Detection:** Machine learning algorithms detect unusual access patterns
- **Incident Response:** Security team investigates all alerts and suspicious activities

13.7 Data Backup & Recovery

Backup Procedures:

- **Frequency:** Full backups are performed daily; incremental backups are performed hourly
- **Encryption:** All backups are encrypted using AES-256 encryption
- **Storage:** Backups are stored in geographically diverse locations within Canada
- **Retention:** Backups are retained for 30 days (daily backups) and 1 year (weekly backups)
- **Testing:** Backup recovery is tested monthly to ensure backups can be restored

Disaster Recovery:

- **Recovery Time Objective (RTO):** CALMSHELL aims to restore services within 4 hours of a disaster
- **Recovery Point Objective (RPO):** Data loss is limited to 1 hour of transactions
- **Disaster Recovery Plan:** A documented plan outlines procedures for responding to major disasters
- **Testing:** Disaster recovery procedures are tested quarterly

13.8 Data Minimization

CALMSHELL collects only the minimum personal information necessary to provide services. Unnecessary data collection is avoided. Users are informed about what data is collected and why.

Data Retention Minimization:

- **Therapy Records:** Retained for 7 years following last session
- **Account Information:** Deleted within 30 days of account closure (except where retention is required by law)
- **Payment Information:** Retained for 7 years for tax and accounting purposes
- **Analytics Data:** De-identified analytics data is retained indefinitely; identified data is deleted after 1 year

13.9 Third-Party Data Processors

CALMSHELL uses third-party service providers (e.g., cloud hosting, payment processing, analytics) that may access user data. All third-party processors are:

- **Contractually Bound:** Data processing agreements require processors to protect data and use it only for specified purposes
- **Audited:** Processors are audited annually for security and compliance
- **Certified:** Processors maintain relevant security certifications (e.g., SOC 2, ISO 27001)
- **Notified:** Users are informed about third-party data processing

13.10 Data Breach Response

If unauthorized access to personal or health information occurs, CALMSHELL follows a structured breach response procedure (see Policy 16: Cybersecurity Incident Response Policy).

13.11 User Data Rights

Users have the following rights regarding their data:

- **Access:** Users may request access to their personal information
- **Correction:** Users may request correction of inaccurate information
- **Deletion:** Users may request deletion of their information (subject to legal retention requirements)
- **Portability:** Users may request their information in a portable format (e.g., CSV, PDF)
- **Withdrawal of Consent:** Users may withdraw consent for data collection and use

---

POLICY 14: CONFIDENTIALITY POLICY

14.1 Purpose & Scope

The Confidentiality Policy establishes standards for maintaining confidentiality of personal and health information. This policy defines who may access information, under what circumstances, and what obligations exist to protect confidentiality.

Confidentiality is a cornerstone of mental health services. Users must be confident that their information will be protected and not disclosed without their consent.

14.2 Confidentiality Obligations

Therapist Confidentiality:

Therapists are bound by professional confidentiality obligations under provincial regulatory standards and professional ethics codes. Therapists must:

- Maintain confidentiality of all information disclosed by clients during therapy
- Not disclose client information to third parties without explicit client consent
- Protect client information from unauthorized access or disclosure
- Maintain confidentiality even after the therapeutic relationship ends
- Comply with legal exceptions to confidentiality (mandatory reporting, court orders)

CALMSHELL Staff Confidentiality:

All CALMSHELL staff members are bound by confidentiality obligations. Staff must:

- Maintain confidentiality of all personal and health information
- Access information only on a need-to-know basis
- Not disclose information to unauthorized persons
- Report confidentiality breaches immediately
- Comply with legal exceptions to confidentiality

Confidentiality Agreements:

All staff members sign confidentiality agreements as a condition of employment. Agreements include:

- Obligation to maintain confidentiality during and after employment
- Penalties for unauthorized disclosure
- Procedures for handling confidential information
- Acknowledgment of legal exceptions to confidentiality

14.3 Authorized Disclosures

With User Consent:

Users may authorize disclosure of their information to:

- Family members or designated contacts
- Other healthcare providers (with specific authorization)
- Insurance companies (for billing purposes)
- Institutional partners (employers, schools) - limited to aggregated data
- Researchers (for research purposes, with specific consent)

Consent must be explicit, informed, and documented. Users may withdraw consent at any time.

Legal Exceptions:

Confidentiality may be breached without user consent in the following circumstances:

- **Mandatory Reporting:** Child abuse, elder abuse, or vulnerable adult abuse must be reported to authorities
- **Court Orders:** Information may be disclosed in response to valid court orders or subpoenas
- **Law Enforcement:** Information may be disclosed to law enforcement in response to valid legal process
- **Imminent Danger:** Information may be disclosed to prevent imminent harm to the user or others
- **Public Health:** Information may be disclosed for public health purposes (e.g., disease reporting)

Disclosure Procedures:

When disclosure is required by law, CALMSHELL:

7 Verifies the validity of the legal request
8 Discloses only the minimum information necessary
9 Notifies the user of the disclosure (unless prohibited by law)
10 Documents the disclosure and reason
11 Maintains records of all disclosures

14.4 Therapist-Client Privilege

Therapist-client privilege is a legal protection that prevents disclosure of communications between therapists and clients in legal proceedings. CALMSHELL:

- Recognizes and protects therapist-client privilege
- Does not disclose privileged communications without user consent or valid legal process
- Advises users of their privilege rights
- Cooperates with legal processes to protect privilege where applicable

14.5 Confidentiality in Virtual Settings

Virtual therapy presents unique confidentiality challenges. CALMSHELL ensures confidentiality by:

- Using encrypted communication channels
- Requiring users to access sessions from private locations
- Requiring therapists to conduct sessions from private locations
- Prohibiting recording without consent
- Limiting access to session information
- Providing guidance on maintaining privacy during virtual sessions

14.6 Confidentiality in Group Settings

When users participate in group therapy or community features, confidentiality is limited. CALMSHELL:

- Informs users that information shared in groups may be seen by other group members
- Requires group members to maintain confidentiality of others' information
- Prohibits recording or sharing of group information without consent
- Monitors groups for confidentiality violations

14.7 Confidentiality Breaches

If confidentiality is breached, CALMSHELL:

12. Investigates the breach immediately
13. Notifies affected users
14. Takes steps to mitigate harm
15. Implements corrective measures to prevent future breaches
16. Documents the breach and response
17. Reports to regulatory authorities if required

14.8 Confidentiality Training

All staff receive confidentiality training covering:

- Legal obligations to maintain confidentiality
- Exceptions to confidentiality
- Procedures for handling confidential information
- Consequences of confidentiality breaches
- Best practices for protecting confidentiality

Training is provided during onboarding and annually thereafter.

14.9 Confidentiality Policies for Institutional Partners

When CALMSHELL partners with institutions (employers, schools, hospitals), confidentiality protections are maintained:

- **Individual Therapy Information:** Not disclosed to institutions without explicit user consent
- **Aggregated Data:** Institutions receive only aggregated, de-identified analytics
- **Institutional Policies:** Institutions must have their own confidentiality policies
- **Data Use Agreements:** Agreements specify permitted uses of data
- **Audit Rights:** CALMSHELL reserves the right to audit institutional use of data

---

POLICY 15: HEALTH INFORMATION RETENTION POLICY

15.1 Purpose & Scope

The Health Information Retention Policy establishes standards for how long personal and health information is retained, how it is stored during retention, and how it is destroyed after the retention period. This policy complies with PHIPA, PIPEDA, professional standards, and legal requirements.

Retention of health information is necessary for continuity of care, legal compliance, and research purposes. However, retention must be limited to necessary periods to minimize privacy risks.

15.2 Retention Periods

Therapy Records & Clinical Documentation:

- **Active Clients:** Retained while client is actively engaged with services
- **Inactive Clients:** Retained for 7 years following the last therapy session
- **Minors:** Retained until age 18, then for 7 additional years (total of 25 years from birth)

- **Postpartum Records:** Retained for 7 years following last session

Retention periods are based on professional standards (e.g., College of Psychologists of Ontario guidelines) and legal requirements.

Account Information:

- **Active Accounts:** Retained while account is active
- **Closed Accounts:** Deleted within 30 days of account closure
- **Exception:** Information retained if required by law or for dispute resolution

Payment & Billing Information:

- **Retained for 7 years** for tax, accounting, and audit purposes
- **Credit card numbers:** Deleted immediately after transaction (not stored)
- **Payment method information:** Retained for subscription management; deleted upon account closure

Assessment Data & Screening Results:

- **Retained for 7 years** following last assessment
- **De-identified data:** Retained indefinitely for research and analytics

Usage & Analytics Data:

- **Identified data:** Deleted after 1 year
- **De-identified data:** Retained indefinitely
- **Cookies & tracking data:** Deleted per cookie policy (typically 1-2 years)

Communication Records:

- **Chat messages:** Retained for 7 years
- **Video recordings:** Retained for 7 years (if recorded with consent)
- **Email communications:** Retained for 7 years

Backup Data:

- **Daily backups:** Retained for 30 days
- **Weekly backups:** Retained for 1 year
- **Backups are encrypted and securely stored**

Legal Holds:

If litigation or investigation is anticipated, information may be retained beyond normal retention periods. Legal holds are documented and tracked.

15.3 Storage During Retention

During the retention period, information is:

- **Encrypted:** All sensitive information is encrypted using AES-256 encryption
- **Secured:** Information is stored on secure servers with access controls
- **Backed Up:** Information is backed up regularly and tested for recovery
- **Monitored:** Access to information is monitored and logged
- **Protected:** Information is protected from loss, theft, or unauthorized access

15.4 Destruction & Deletion

After the retention period expires, information is destroyed using secure methods:

Digital Data Destruction:

- **Secure Deletion:** Data is deleted using secure deletion tools that overwrite data multiple times
- **Encryption Key Destruction:** Encryption keys are destroyed, rendering encrypted data unrecoverable
- **Database Purging:** Database records are purged and verified as deleted
- **Backup Destruction:** Backups containing deleted data are destroyed

Physical Data Destruction:

- **Hard Drive Destruction:** Hard drives containing sensitive data are physically destroyed (shredding, degaussing)
- **Paper Records:** Paper records are shredded or incinerated
- **Certification:** Destruction is certified and documented

De-Identification:

Before deletion, information may be de-identified for research or analytics purposes. De-identification removes identifiers (name, contact information, government ID) so data cannot be linked to individuals.

15.5 User Requests for Deletion

Users may request deletion of their information at any time. CALMSHELL will delete information within 30 days, except:

- **Legal Requirements:** Information required by law is retained
- **Dispute Resolution:** Information may be retained for dispute resolution

- **Backup Data:** Information in backups is deleted per backup retention schedule
- **De-Identified Data:** De-identified data may be retained indefinitely

Users are notified of deletion and provided confirmation.

15.6 Retention Schedule

CALMSHELL maintains a detailed retention schedule that documents:

- Type of information
- Retention period
- Legal/regulatory basis for retention
- Storage location and security measures
- Destruction method and timeline
- Responsible party for retention and destruction

The retention schedule is reviewed annually and updated as needed.

15.7 Retention Compliance Monitoring

CALMSHELL monitors compliance with retention policies through:

- **Automated Deletion:** Automated systems delete information at the end of retention periods
- **Quarterly Audits:** Quarterly audits verify that information is deleted per schedule
- **Destruction Certification:** Destruction is certified and documented
- **Exception Tracking:** Exceptions to retention policies are tracked and justified

15.8 Institutional Partner Retention

When CALMSHELL partners with institutions, retention policies are specified in data use agreements:

- **Aggregated Data:** Institutions may retain aggregated, de-identified data indefinitely
- **Individual Data:** Institutions must delete individual data per CALMSHELL retention schedule
- **Audit Rights:** CALMSHELL reserves the right to audit institutional retention

15.9 Retention During Disputes

If a user disputes charges or raises a complaint, information may be retained beyond normal retention periods for dispute resolution. Retention during disputes is:

- **Limited:** Retained only as long as necessary for dispute resolution

- **Documented:** Documented with the reason for retention
- **Destroyed:** Destroyed once dispute is resolved

POLICY 16: CYBERSECURITY INCIDENT RESPONSE POLICY

16.1 Purpose & Scope

The Cybersecurity Incident Response Policy establishes procedures for identifying, responding to, and managing cybersecurity incidents, including data breaches, ransomware attacks, system outages, and other security events. This policy ensures that incidents are detected quickly, responded to effectively, and disclosed appropriately.

16.2 Incident Classification

CALMSHELL classifies incidents by severity:

Critical Incidents (Severity 1):

- Confirmed data breach involving health information
- Ransomware attack affecting critical systems
- Complete platform outage
- Unauthorized access to user accounts
- Compromise of encryption keys

High Incidents (Severity 2):

- Suspected data breach (under investigation)
- Partial platform outage (>1 hour)
- Unauthorized access to non-sensitive systems
- Malware detected on systems
- Denial-of-service attack

Medium Incidents (Severity 3):

- Failed authentication attempts
- Suspicious access patterns
- Minor system vulnerabilities
- Partial data loss (recoverable)
- Brief service disruption (<1 hour)

Low Incidents (Severity 4):

- Failed login attempts (normal volume)
- Minor security alerts
- Outdated software (non-critical)
- Low-risk vulnerabilities

16.3 Incident Detection

CALMSHELL detects incidents through:

Automated Monitoring:

- **Intrusion Detection Systems (IDS):** Monitor network traffic for suspicious activity
- **Endpoint Detection & Response (EDR):** Monitor devices for malware and suspicious behavior
- **Security Information & Event Management (SIEM):** Aggregate and analyze security logs
- **Vulnerability Scanning:** Regular scans identify security weaknesses
- **Penetration Testing:** Quarterly testing simulates attacks to identify vulnerabilities

User Reports:

- Users may report suspected security incidents through security@calmshell.ca
- Reports are investigated immediately

Third-Party Notifications:

- Payment processors, cloud providers, and other partners notify CALMSHELL of incidents
- Notifications are investigated immediately

16.4 Incident Response Procedures

Immediate Response (0-1 hour):

18. **Activate Incident Response Team:** Security team is notified immediately
19. **Classify Incident:** Incident is classified by severity
20. **Isolate Affected Systems:** Compromised systems are isolated to prevent spread
21. **Preserve Evidence:** Logs, memory, and other evidence are preserved for investigation
22. **Notify Leadership:** Executive team is notified of critical incidents
23. **Establish Communication:** Incident response team establishes communication channels

Investigation (1-24 hours):

24 **Determine Scope:** Investigate what information was accessed and how many users affected
25 **Identify Root Cause:** Determine how the incident occurred
26 **Assess Impact:** Evaluate impact on users, operations, and reputation
27 **Collect Evidence:** Gather logs, forensic data, and other evidence
28 **Notify Authorities:** Report to law enforcement if criminal activity suspected
29 **Consult Experts:** Engage external cybersecurity experts if needed

Containment (1-7 days):

30 **Patch Vulnerabilities:** Apply security patches to prevent recurrence
31 **Reset Credentials:** Reset passwords and authentication tokens if compromised
32 **Enhance Monitoring:** Increase monitoring for signs of ongoing attack
33 **Communicate with Users:** Notify users of incident and recommended actions
34 **Implement Safeguards:** Implement additional security measures

Recovery (1-30 days):

35 **Restore Systems:** Restore compromised systems from clean backups
36 **Verify Integrity:** Verify that systems are functioning correctly
37 **Monitor for Recurrence:** Monitor for signs of repeat attacks
38 **Conduct Post-Mortem:** Analyze incident to identify lessons learned
39 **Implement Improvements:** Implement improvements to prevent future incidents

Communication (Ongoing):

40 **User Notification:** Users are notified of breaches per legal requirements
41 **Regulatory Notification:** Regulatory authorities are notified per legal requirements
42 **Public Communication:** Public statements are issued if appropriate
43 **Ongoing Updates:** Users are provided with updates on incident status and remediation

16.5 Data Breach Notification

If a data breach occurs involving personal or health information, CALMSHELL notifies affected users and regulatory authorities:

User Notification:

- **Timing:** Notification is provided without unreasonable delay, typically within 10 business days
- **Content:** Notification includes:
    - Description of the breach
    - Information that may have been accessed

    - Steps CALMSHELL is taking to address the breach
    - Recommended actions for users (e.g., monitor credit, change passwords)
    - Contact information for questions
- **Method:** Notification is provided via email, SMS, or in-app notification
- **Language:** Notification is provided in plain language

Regulatory Notification:

- **Privacy Commissioner:** Breach is reported to the Office of the Privacy Commissioner of Canada if personal information is affected
- **Health Authorities:** Breach is reported to provincial health authorities if health information is affected
- **Law Enforcement:** Breach is reported to law enforcement if criminal activity is suspected

Documentation:

- Breach is documented including date, scope, impact, and response
- Documentation is retained for at least 2 years

16.6 Ransomware Response

If ransomware is detected, CALMSHELL follows specific procedures:

44 **Isolate Systems:** Infected systems are immediately isolated to prevent spread
45 **Do Not Pay:** CALMSHELL does not pay ransoms
46 **Preserve Evidence:** Evidence is preserved for law enforcement
47 **Restore from Backups:** Systems are restored from clean backups
48 **Notify Authorities:** Law enforcement is notified
49 **Notify Users:** Users are notified if their data may have been accessed

16.7 Denial-of-Service (DoS) Response

If a denial-of-service attack occurs, CALMSHELL:

50 **Detect Attack:** Automated systems detect unusual traffic patterns
51 **Activate DDoS Mitigation:** DDoS mitigation services are activated
52 **Route Traffic:** Traffic is routed through DDoS mitigation providers
53 **Communicate Status:** Users are informed of service status
54 **Investigate Source:** Investigation identifies attack source
55 **Implement Countermeasures:** Firewall rules and other countermeasures are implemented

16.8 Third-Party Incident Response

If a third-party service provider (cloud host, payment processor) experiences a security incident, CALMSHELL:

56 **Assess Impact:** Determine if CALMSHELL or user data is affected
57 **Notify Users:** Users are notified if their data is affected
58 **Implement Safeguards:** Additional safeguards are implemented
59 **Review Contracts:** Service provider contracts are reviewed for breach notification requirements
60 **Audit Provider:** Provider is audited to verify incident response

16.9 Business Continuity & Disaster Recovery

CALMSHELL maintains business continuity and disaster recovery procedures:

Recovery Time Objective (RTO): Services are restored within 4 hours of a major incident

Recovery Point Objective (RPO): Data loss is limited to 1 hour of transactions

Disaster Recovery Plan: A documented plan outlines procedures for responding to major disasters

Testing: Disaster recovery procedures are tested quarterly

Backup Systems: Redundant systems and backups ensure continuity

16.10 Incident Response Training

All staff receive incident response training covering:

- Incident classification and reporting
- Incident response procedures
- Role-specific responsibilities
- Communication procedures
- Evidence preservation
- Legal and regulatory requirements

Training is provided during onboarding and annually thereafter.

16.11 Post-Incident Review

After each incident, CALMSHELL conducts a post-incident review:

61 **Timeline:** Document incident timeline and response actions
62 **Root Cause:** Identify root cause of incident
63 **Impact:** Assess impact on users, operations, and reputation
64 **Response Effectiveness:** Evaluate effectiveness of incident response
65 **Lessons Learned:** Identify lessons learned
66 **Recommendations:** Make recommendations for improvement
67 **Implementation:** Implement recommendations to prevent future incidents

16.12 Incident Response Team

CALMSHELL maintains an Incident Response Team responsible for:

- **Detection:** Monitoring for security incidents
- **Response:** Responding to incidents per procedures
- **Investigation:** Investigating incidents to determine root cause
- **Communication:** Communicating with users, authorities, and stakeholders
- **Recovery:** Recovering from incidents
- **Improvement:** Implementing improvements to prevent future incidents

Team Composition:

- Chief Information Security Officer (CISO)
- Security Operations Center (SOC) Manager
- Incident Response Coordinator
- System Administrators
- Database Administrators
- Legal Counsel
- Communications Manager
- Clinical Director (for health-related incidents)

16.13 Incident Response Plan Documentation

CALMSHELL maintains detailed incident response plan documentation including:

- Incident classification procedures
- Detection methods and tools
- Response procedures for each incident type
- Communication templates
- Contact lists for internal and external parties
- Legal and regulatory requirements
- Testing and training schedule

Documentation is reviewed and updated annually.

IMPLEMENTATION CHECKLISTS

Checklist 13: Data Protection & Encryption Implementation

Task	Responsible Party	Deadline	Status
Conduct data classification audit	IT Security Team	Week 1	☐
Document all data types and sensitivity	Privacy Officer	Week 1	☐
Review current encryption standards	IT Security Team	Week 1	☐
Implement TLS 1.2+ for all web traffic	IT Infrastructure	Week 2	☐
Implement certificate pinning in mobile apps	Mobile Development	Week 2	☐
Implement AES-256 encryption for databases	Database Team	Week 2-3	☐
Implement file system encryption	IT Infrastructure	Week 3	☐
Establish key management system	IT Security Team	Week 3	☐
Implement key rotation procedures	IT Security Team	Week 3	☐
Verify Canadian data residency	IT Infrastructure	Week 4	☐
Implement access control system	IT Security Team	Week 4	☐
Implement MFA for all staff	IT Infrastructure	Week 4	☐
Implement audit logging	IT Infrastructure	Week 4	☐
Implement backup encryption	Backup Team	Week 4	☐

Task	Responsible Party	Deadline	Status
Test backup recovery procedures	Backup Team	Week 5	☐
Document encryption standards	IT Security Team	Week 5	☐
Train staff on data protection	IT Security Team	Week 5	☐

Checklist 14: Confidentiality Implementation

Task	Responsible Party	Deadline	Status
Draft Confidentiality Policy	Legal Team	Week 1	☐
Review with clinical advisors	Clinical Team	Week 1	☐
Create confidentiality agreements	Legal Team	Week 2	☐
Implement confidentiality training	HR Team	Week 2	☐
Train all staff on confidentiality	HR Team	Week 2-3	☐
Create disclosure procedures	Legal Team	Week 2	☐
Implement access controls	IT Security Team	Week 3	☐
Create legal hold procedures	Legal Team	Week 3	☐
Develop therapist-client privilege procedures	Legal Team	Week 3	☐
Create breach notification procedures	Legal Team	Week 4	☐
Implement group confidentiality guidelines	Product Team	Week 4	☐
Create institutional partner agreements	Legal Team	Week 4	☐

Task	Responsible Party	Deadline	Status
Document confidentiality procedures	Compliance Team	Week 5	☐

Checklist 15: Health Information Retention Implementation

Task	Responsible Party	Deadline	Status
Develop retention schedule	Compliance Team	Week 1	☐
Document retention periods by data type	Privacy Officer	Week 1	☐
Implement automated deletion system	IT Development	Week 2	☐
Create retention policy documentation	Compliance Team	Week 2	☐
Implement secure deletion procedures	IT Security Team	Week 2-3	☐
Create destruction certification procedures	Compliance Team	Week 3	☐
Implement backup retention schedule	Backup Team	Week 3	☐
Create user deletion request procedures	Support Team	Week 3	☐
Implement legal hold procedures	Legal Team	Week 4	☐
Create retention audit procedures	Compliance Team	Week 4	☐
Train staff on retention procedures	Compliance Team	Week 4	☐
Create institutional partner retention agreements	Legal Team	Week 4	☐
Document retention compliance monitoring	Compliance Team	Week 5	☐

Checklist 16: Cybersecurity Incident Response Implementation

Task	Responsible Party	Deadline	Status
Develop incident response plan	IT Security Team	Week 1	☐
Create incident classification procedures	IT Security Team	Week 1	☐
Establish Incident Response Team	CISO	Week 1	☐
Implement intrusion detection system (IDS)	IT Infrastructure	Week 2	☐
Implement endpoint detection & response (EDR)	IT Security Team	Week 2	☐
Implement SIEM system	IT Security Team	Week 2-3	☐
Create incident response procedures	IT Security Team	Week 2	☐
Create communication templates	Communications Team	Week 2	☐
Create user notification procedures	Communications Team	Week 3	☐
Create regulatory notification procedures	Legal Team	Week 3	☐
Implement ransomware response procedures	IT Security Team	Week 3	☐
Implement DDoS mitigation	IT Infrastructure	Week 3	☐
Create business continuity plan	Operations Team	Week 3-4	☐
Create disaster recovery plan	IT Infrastructure	Week 4	☐
Test disaster recovery procedures	IT Infrastructure	Week 4	☐
Create incident response training program	IT Security Team	Week 4	☐

Task	Responsible Party	Deadline	Status
Train all staff on incident response	IT Security Team	Week 5	☐
Create post-incident review procedures	IT Security Team	Week 5	☐
Document incident response plan	IT Security Team	Week 5	☐

COMPLIANCE TRACKING

Compliance Tracking Matrix

Policy	Regulatory Requirement	Compliance Status	Evidence	Last Reviewed	Next Review
Data Protection & Encryption	PIPEDA, PHIPA, CASL	☐ Compliant	Encryption audit, key management procedures	[Date]	[Date]
Confidentiality	PHIPA, Professional Standards, Common Law	☐ Compliant	Confidentiality agreements, training records	[Date]	[Date]
Health Information Retention	PHIPA, Professional Standards	☐ Compliant	Retention schedule, destruction certification	[Date]	[Date]
Cybersecurity Incident Response	PIPEDA, PHIPA, Breach Notification Laws	☐ Compliant	Incident response plan, testing records	[Date]	[Date]

Compliance Review Schedule

Quarterly Reviews: Incident response procedures, access control audits, encryption key rotation
Semi-Annual Reviews: Data protection standards, confidentiality procedures, retention compliance
Annual Reviews: All policies, regulatory landscape assessment, security testing

Responsible Parties

Role	Responsibilities
Chief Information Security Officer (CISO)	Overall cybersecurity strategy, incident response
Privacy Officer	Data protection, confidentiality, retention
IT Security Team	Encryption, access control, monitoring
IT Infrastructure Team	System security, backups, disaster recovery
Legal Counsel	Legal compliance, breach notification, regulatory reporting
Compliance Manager	Compliance tracking, audit coordination
Incident Response Team	Incident detection, response, investigation

---

SECURITY STANDARDS & FRAMEWORKS

CALMSHELL aligns with industry-standard security frameworks:

ISO 27001: Information Security Management System
NIST Cybersecurity Framework: Risk management and incident response
CIS Controls: Critical security controls and best practices
OWASP Top 10: Web application security
SOC 2 Type II: Service organization controls and trust services criteria

---

CONTINUOUS IMPROVEMENT

CALMSHELL is committed to continuous improvement of security practices:

- **Quarterly Security Reviews:** Review security posture and identify improvements
- **Annual Penetration Testing:** Conduct comprehensive security testing

- **Vulnerability Management:** Identify and remediate vulnerabilities promptly
- **Security Training:** Provide regular training to staff on security best practices
- **Incident Analysis:** Analyze incidents to identify root causes and prevent recurrence
- **Technology Updates:** Stay current with security technology and best practices

---

Document Status: Draft for Implementation
Prepared By: CALMSHELL IT Security & Compliance Team
Date: June 2026
Version: 1.0