Document Control

Document Information	Details
Document Title	C6Med, LLC Written Information Security Program (WISP)
Document Version	1.0
Document Status	Draft
Document Owner	Vikas Bhatia
Prepared By	Vikas Bhatia
Prepared Date	April 23, 2025
Approved By	Pending
Approved Date	Pending

Version History

Version	Date	Author	Description of Changes
0.1	April 23, 2025	Vikas Bhatia	Initial draft
1.0	April 23, 2025	Vikas Bhatia	Final document

---

1. Position Statement

C6Med, LLC Information Security Commitment

C6Med, LLC is committed to safeguarding the confidentiality, integrity, and availability of all information assets and systems entrusted to us. As a medical communications partner to leading pharmaceutical companies, we understand the sensitivity of the information we handle and the importance of maintaining the highest security standards.

Our Information Security Program is aligned with the NIST Cybersecurity Framework (CSF) and is designed to:

- Protect client information through appropriate technical, administrative, and physical safeguards
- Ensure compliance with all applicable contractual obligations, laws, and regulations
- Provide secure and reliable services to our partners and clients
- Continuously evaluate and improve our security posture to address evolving threats
- Foster a culture of security awareness throughout our organization

We are dedicated to transparent communication with our clients and partners regarding our security practices and will promptly address any security concerns that may arise. Through our ongoing commitment to information security, C6Med, LLC aims to maintain the trust our clients have placed in us as their valued medical communications partner.

Approved by:

Marcy Duval
Owner/Leader, C6Med, LLC
Date: _________________

---

2. Information Security Policy

C6Med, LLC Information Security Policy

Purpose and Scope

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of C6Med, LLC's information assets. This policy applies to all employees, contractors, temporary workers, and third parties who have access to C6Med, LLC information resources.

Policy Statement

C6Med, LLC is committed to:

1. Protecting client information by implementing appropriate security controls
2. Complying with all contractual, legal, and regulatory requirements

3. Maintaining business continuity through proper information security practices
4. Continuous improvement of our information security program

Roles and Responsibilities

Leadership Responsibilities

- Ensure adequate resources are allocated to information security
- Review and approve information security policies and procedures
- Promote a culture of information security awareness
- Oversee the implementation of security controls

Employee/Contractor Responsibilities

- Comply with all information security policies and procedures
- Report security incidents promptly
- Participate in security awareness training
- Protect information assets from unauthorized access, disclosure, or modification
- Adhere to the Acceptable Use Policy

Information Classification

All information shall be classified based on its sensitivity and importance:

1. **Confidential**: Highly sensitive client data, medical expert information, proprietary business information
2. **Internal**: Non-sensitive information intended for internal use only
3. **Public**: Information approved for public release

Risk Management

C6Med, LLC will:

- Perform regular risk assessments
- Implement controls to mitigate identified risks
- Document and track risks in the company risk register
- Review and update risk assessments annually or upon significant change

Access Control

- Access to information assets shall be granted based on the principle of least privilege
- Regular access reviews will be conducted
- Passwords must meet complexity requirements
- Multi-factor authentication shall be used for accessing sensitive information

Data Security

- Sensitive information must be encrypted during transmission
- All devices accessing company information must be encrypted
- Data sharing must follow established procedures
- Information must be securely disposed of when no longer needed

Incident Response

- All security incidents must be reported immediately
- A formal incident response process will be followed
- Documentation of incidents will be maintained
- Lessons learned will be incorporated into security practices

Compliance and Enforcement

- Regular compliance reviews will be conducted
- Non-compliance may result in disciplinary action
- Third-party service providers must comply with our security requirements
- Annual security awareness training is mandatory for all personnel

Policy Review

This policy shall be reviewed annually or upon significant changes to the business environment.

Approved by:

Marcy Duval
Owner/Leader, C6Med, LLC
Date: _________________

---

3. Acceptable Use Policy

C6Med, LLC Acceptable Use Policy

Purpose

This Acceptable Use Policy defines the appropriate use of C6Med, LLC's information technology resources, including devices, networks, applications, and data.

User Responsibilities

Device Security

- Keep all devices used for C6Med, LLC business secure with:
  - Full-disk encryption
  - Current antivirus/anti-malware software
  - Regular system updates (at minimum, weekly)
  - Strong password/PIN protection
  - Automatic screen locks after 15 minutes of inactivity
- Never leave devices unattended in public places
- Report lost or stolen devices immediately

Password Management

- Use unique, complex passwords for all accounts
- Change passwords every 90 days
- Use the company-provided password manager
- Enable two-factor authentication (2FA) for all business applications
- Never share passwords with others
- Never use C6Med, LLC passwords for personal accounts

Email and Communications

- Exercise caution with email attachments and links
- Verify the sender before responding to requests for sensitive information
- Mark suspicious emails as spam and report them to management
- Never forward confidential information to personal email accounts
- Use secure methods for sharing sensitive information
- Avoid discussing confidential information in public areas

Data Handling

- Store business data only in approved locations (SharePoint/Office 365)
- Avoid using personal storage services for business data
- Classify information according to sensitivity
- Only share information on a need-to-know basis
- Securely dispose of sensitive information when no longer needed
- Verify recipient identity before sharing sensitive information

Remote Work

- Use company VPN when connecting to public Wi-Fi
- Avoid using public computers for business activities
- Ensure home networks are secured with strong passwords
- Keep work areas private to prevent unauthorized viewing of information

- Lock devices when stepping away, even at home

Software and Applications

- Only install approved software on devices used for business
- Keep software updated with the latest security patches
- Do not disable security features or controls
- Use only licensed software and respect copyright laws
- Report any suspicious software behavior

Social Media and Internet Use

- Exercise good judgment when posting online
- Never share confidential client information on social media
- Do not speak on behalf of C6Med, LLC without authorization
- Be aware that online activities may reflect on the company

Incident Reporting

- Report any security incidents or concerns immediately
- Examples of incidents include:
  - Suspected phishing emails
  - Lost or stolen devices
  - Unauthorized access attempts
  - Accidental data disclosure
  - Malware infections

Compliance

All users must acknowledge receipt and understanding of this policy. Violations may result in disciplinary action, up to and including termination of employment or contract.

I acknowledge that I have read and understand the C6Med, LLC Acceptable Use Policy and agree to comply with all its provisions.

Name: ____________________

Signature: ____________________

Date: ____________________

---

4. Standard Operating Procedures (SOP)

C6Med, LLC Information Security Standard Operating Procedures

SOP-01: Security Governance

Purpose

This procedure establishes the governance structure for C6Med, LLC's information security program.

Procedure

1. **Security Team Structure**
    - Security Owner: Marcy Duval (Owner/Leader)
    - Security Lead: [Designated Security Lead]
    - Team Members: All employees and contractors
2. **Meetings and Reporting**
    - Monthly security status review meetings
    - Quarterly risk assessment reviews
    - Annual comprehensive security program assessment
3. **Documentation Management**
    - All security documentation to be stored in SharePoint
    - Version control maintained for all security documents
    - Annual review of policies and procedures
4. **Metrics and Reporting**
    - Track security incidents
    - Monitor compliance with security requirements
    - Report on training completion rates
    - Track remediation of identified vulnerabilities

SOP-02: Risk Management

Purpose

This procedure defines the process for identifying, assessing, and managing information security risks.

Procedure

1. **Risk Assessment**
    - Conduct formal risk assessments annually
    - Document risks in the Risk Register
    - Assess likelihood and impact using defined criteria

    - Calculate risk ratings based on likelihood and impact
2. **Risk Treatment**
    - For each identified risk, select treatment option:
        - Mitigate: Implement controls to reduce risk
        - Transfer: Share risk through insurance or third parties
        - Accept: Formally accept risks below threshold
        - Avoid: Eliminate risk by removing cause
    - Document rationale for selected treatment options
3. **Risk Monitoring**
    - Review Risk Register quarterly
    - Update risk status based on control implementation
    - Reassess risks when business changes occur
    - Report significant risk changes to leadership

SOP-03: Asset Management

Purpose

This procedure establishes requirements for managing information assets.

Procedure

1. **Asset Inventory**
    - Maintain inventory of all hardware, software, and data assets
    - Record asset owner, location, classification, and status
    - Update inventory quarterly or upon significant changes
    - Verify inventory accuracy annually
2. **Asset Classification**
    - Classify all information assets according to sensitivity
    - Apply appropriate controls based on classification
    - Review and update classifications annually
    - Label sensitive information appropriately
3. **Asset Handling**
    - Define procedures for each asset classification
    - Document access restrictions for sensitive assets
    - Establish procedures for secure asset disposal
    - Implement change management for critical assets
4. **Information Repository Management**
    - Consolidate all company files in SharePoint/Office 365

- Decommission Dropbox after migration and cleanup
- Utilize version control capabilities for critical documents
- Implement automated backup procedures for documents in client environments
- Maintain regular audits of repository access rights

SOP-04: Access Management

Purpose

This procedure defines requirements for managing access to information systems.

Procedure

1. **Account Provisioning**
   - Document required access for each role
   - Implement formal access request process
   - Require manager approval for all access requests
   - Provision minimum necessary access rights
   - Select appropriate license types based on job requirements
2. **Access Review**
   - Conduct quarterly access reviews
   - Remove unnecessary access rights
   - Update access when roles change
   - Document completed reviews
   - Utilize SharePoint access audit reports
   - Review folder-level permissions in SharePoint
3. **Account Termination**
   - Implement offboarding checklist for departing personnel
   - Remove access within 24 hours of termination
   - Recover company assets from departing personnel
   - Maintain records of completed termination actions
4. **SharePoint Permission Management**
   - Establish clear ownership for each SharePoint area
   - Document and implement folder-level access controls
   - Regularly audit SharePoint permissions using automated reports
   - Implement approval workflow for permission changes
   - Maintain documentation of permission structures

SOP-05: Security Awareness

Purpose

This procedure establishes requirements for security awareness training.

Procedure

1. **Training Program**
    - Deliver initial security training during onboarding
    - Provide annual refresher training
    - Conduct targeted training for specific roles
    - Test comprehension through quizzes or exercises
2. **Awareness Communications**
    - Send monthly security awareness communications
    - Share relevant security news and updates
    - Provide practical security tips
    - Recognize positive security behaviors
3. **Phishing Simulation**
    - Conduct quarterly phishing simulations
    - Provide immediate feedback on failures
    - Track improvement over time
    - Deliver remedial training for repeated failures

SOP-06: Incident Response

Purpose

This procedure defines the process for responding to security incidents.

Procedure

1. **Incident Detection**
    - Establish methods for detecting potential incidents
    - Define criteria for classifying incidents
    - Document reporting channels
    - Train personnel on incident recognition
2. **Incident Response Steps**
    - Containment: Limit incident impact
    - Eradication: Remove cause of incident
    - Recovery: Restore affected systems
    - Lessons Learned: Document and improve
3. **Incident Documentation**

    - Record all incident details
    - Document response actions taken
    - Track time to resolution
    - Update procedures based on lessons learned

SOP-07: Business Continuity

Purpose

This procedure establishes requirements for ensuring business continuity.

Procedure

1. **Backup Management**
    - Implement automated backups for critical data
    - Test backup restoration quarterly
    - Store backups securely with encryption
    - Document backup schedules and retention periods
    - Establish automated backup procedures for client-shared documents
2. **Version Control Management**
    - Implement version control for all critical documents
    - Automate backup of documents shared in client environments
    - Establish regular cadence for document preservation
    - Provide training on version history features in all platforms
    - Document procedures for restoring previous versions
3. **Recovery Planning**
    - Identify critical business functions
    - Establish recovery time objectives
    - Document recovery procedures
    - Test recovery processes annually
4. **Alternative Work Arrangements**
    - Define procedures for remote work during disruptions
    - Establish communication protocols during incidents
    - Document emergency contact information
    - Test alternative work procedures annually

SOP-08: Vendor Management

Purpose

This procedure defines requirements for managing security with third-party vendors.

Procedure

1. **Vendor Assessment**
    - Assess vendor security before engagement
    - Document vendor security requirements
    - Include security requirements in contracts
    - Maintain inventory of vendor relationships
2. **Ongoing Monitoring**
    - Review vendor security annually
    - Monitor for vendor security incidents
    - Verify compliance with contractual requirements
    - Update vendor security requirements as needed
3. **Vendor Termination**
    - Define security requirements for vendor termination
    - Ensure return or destruction of company data
    - Revoke vendor access to systems
    - Document completion of termination activities

SOP-09: Compliance Management

Purpose

This procedure establishes requirements for managing compliance with regulatory and contractual obligations.

Procedure

1. **Compliance Inventory**
    - Maintain inventory of applicable requirements
    - Map requirements to security controls
    - Review compliance status quarterly
    - Document evidence of compliance
2. **Compliance Assessment**
    - Conduct annual self-assessment
    - Address identified compliance gaps
    - Prepare for external assessments
    - Document completed assessments
3. **Monitoring Changes**
    - Track changes to regulatory requirements

- Update security controls as needed
- Communicate changes to affected personnel
- Maintain compliance documentation

SOP-10: Continuous Improvement

Purpose

This procedure defines the process for continuously improving the security program.

Procedure

1. **Program Review**
   - Conduct annual security program assessment
   - Benchmark against industry standards
   - Identify improvement opportunities
   - Document recommendations
2. **Implementation Planning**
   - Prioritize improvement initiatives
   - Allocate resources for implementation
   - Establish timelines and milestones
   - Track implementation progress
3. **Effectiveness Measurement**
   - Define metrics for measuring effectiveness
   - Collect and analyze metric data
   - Report results to leadership
   - Adjust program based on results

SOP-11: Communication Tools Management

Purpose

This procedure establishes guidelines for managing communication tools within C6Med, LLC.

Procedure

1. **Tool Selection and Usage**
   - Use Slack for internal team communications
   - Use client Teams environments exclusively for client communications
   - Never mix client and internal communications across platforms
   - Document approved tools and their specific purposes

2. **Calendar Management**
   - Configure calendar sharing permissions for team visibility
   - Ensure calendar topics are appropriately visible to internal team
   - Apply privacy settings for client-specific calendar items
   - Maintain consistent calendar practices across browser and desktop applications
3. **Distribution List Management**
   - Maintain separate internal and external distribution lists
   - Document procedures for creating and updating distribution lists
   - Review distribution list permissions quarterly
   - Implement naming conventions for distribution lists
4. **Communication Security**
   - Encrypt sensitive communications
   - Verify recipient identities before sharing sensitive information
   - Apply appropriate data classification to communications
   - Review communication tools security settings quarterly# C6Med, LLC Written Information Security Program (WISP)