HATCH LABS HOLDINGS LLC
INFORMATION SECURITY POLICY

Document Version: 1.0
Effective Date: March 6, 2026
Next Review: March 6, 2027
Document Owner: CEO

---

1. PURPOSE AND SCOPE

1.1 Purpose
This Information Security Policy establishes the framework for protecting Hatch Labs Holdings LLC's information assets, systems, and data. This policy ensures the confidentiality, integrity, and availability of information and supports compliance with applicable legal, regulatory, and contractual requirements.

1.2 Scope
This policy applies to all employees, contractors, consultants, business partners, and third parties who access Hatch Labs systems, networks, or data. It covers all information systems, applications, networks, and data owned or operated by Hatch Labs Holdings LLC, including the AmandasList platform.

1.3 Company Overview
• **Legal Entity:** Hatch Labs Holdings LLC (Delaware LLC, EIN 39-2892314)
• **Primary Product:** AmandasList — a verified membership network for high-achieving professionals
• **Business Address:** 701 Tillery Street, Suite 12, Austin TX 78702
• **Contact:** amanda@hatchlabs.com
• **Website:** amandaslist.com, hatchlabs.com
• **CEO:** Amanda Bradford

---

2. ROLES AND RESPONSIBILITIES

2.1 Chief Executive Officer (Chief Security Officer)
As a solo founder startup, the CEO serves as the primary security officer and is responsible for:
• Overall information security governance and strategy
• Approval of security policies and procedures
• Security incident escalation and decision-making

• Annual security policy review and updates
• Security vendor selection and management
• Budget allocation for security initiatives

2.2 Development Team (Currently CEO)
Responsible for:
• Secure coding practices
• Implementation of security controls in applications
• Security testing and vulnerability assessments
• Security configuration management
• Incident response technical activities

2.3 All Personnel and Contractors
Responsible for:
• Complying with security policies and procedures
• Reporting security incidents and suspicious activities
• Protecting company information and systems
• Maintaining confidentiality of sensitive information
• Participating in security awareness activities

---

3. ACCESS CONTROL AND IDENTITY MANAGEMENT

3.1 User Access Management
• **Principle of Least Privilege:** Users are granted minimum access necessary to perform their job functions
• **Role-Based Access Control (RBAC):** Access permissions are assigned based on predefined roles and responsibilities
• **Regular Access Reviews:** User access is reviewed quarterly and adjusted based on role changes or termination

3.2 Multi-Factor Authentication (MFA)
Mandatory MFA is required for:
• All critical systems (Supabase, Google Workspace, Mercury Bank)
• User access to Plaid Link for identity verification
• Administrative access to any system containing user data
• Remote access to company resources

3.3 Account Management
• Unique user accounts for each individual
• Strong password requirements (minimum 12 characters, complexity requirements)
• Account lockout policies after failed login attempts

• Immediate account deactivation upon termination or role change
• Shared accounts are prohibited

3.4 Privileged Access Management
• Administrative accounts are separate from standard user accounts
• Privileged access is monitored and logged
• Administrative activities require dual approval where technically feasible
• Regular review of privileged account holders

---

4. DATA CLASSIFICATION AND HANDLING

4.1 Data Classification Levels

PUBLIC: Information intended for public disclosure (marketing materials, public website content)

INTERNAL: Information for internal business use (internal policies, business plans, non-sensitive operational data)

CONFIDENTIAL: Sensitive business information requiring protection (user data, financial information, business intelligence, vendor contracts)

RESTRICTED: Highly sensitive information requiring the highest level of protection (authentication credentials, encryption keys, sensitive personal data, financial account data)

4.2 Data Handling Requirements
• Data must be labeled according to classification level
• Handling procedures must match the sensitivity level
• Data sharing requires approval based on classification
• Secure disposal required for all confidential and restricted data
• Data retention periods defined by classification and legal requirements

4.3 Personal Data Protection
Given AmandasList's collection of personal and financial data through Plaid:
• All personal data classified as Confidential or Restricted
• Financial account data classified as Restricted
• Identity verification data classified as Restricted
• Special handling procedures for financial data per applicable regulations

---

5. ENCRYPTION STANDARDS

5.1 Data Encryption at Rest
• **Primary Database:** AES-256 encryption via Supabase hosted PostgreSQL
• **Minimum Standard:** AES-256 encryption for all databases containing personal or financial data
• **Key Management:** Encryption keys managed by Supabase with industry-standard key rotation
• **Scope:** All user data, financial data from Plaid, identity verification data, and business-critical information

5.2 Data Encryption in Transit
• **Minimum Standard:** TLS 1.2 or higher for all data in transit
• **Implementation:** TLS 1.3 where supported, with perfect forward secrecy
• **API Communications:** All API calls to third-party services (Plaid, Supabase) use TLS 1.2+
• **Web Application:** HTTPS enforced with HSTS headers
• **Certificate Management:** Automated certificate renewal via Cloudflare

5.3 Encryption Implementation
• Strong cipher suites only (AES-256, ChaCha20-Poly1305)
• Weak encryption protocols explicitly disabled (SSL, TLS 1.0, TLS 1.1)
• Regular assessment of encryption implementation
• Compliance with current cryptographic best practices

---

6. INCIDENT RESPONSE PROCEDURES

6.1 Incident Response Team
• **Incident Commander:** CEO (Amanda Bradford)
• **Technical Lead:** Development team lead (currently CEO)
• **External Resources:** Cybersecurity consultant (as needed)
• **Legal Counsel:** External legal counsel (as needed)

6.2 Incident Classification
• **Low:** Minor security violations with minimal impact
• **Medium:** Security incidents with potential business impact
• **High:** Major security breaches affecting user data or business operations
• **Critical:** Severe breaches involving financial data or system compromise

6.3 Response Procedures
1. **Detection and Analysis** (0-1 hour)
   - Identify and verify the incident

- Assess scope and potential impact
- Document initial findings

2. **Containment** (1-4 hours)
- Immediate containment of the incident
- Prevent further damage or data loss
- Preserve evidence for investigation

3. **Eradication and Recovery** (4-24 hours)
- Remove threat and vulnerabilities
- Restore systems and data from backups
- Implement additional security measures

4. **Post-Incident Activities** (24-72 hours)
- Conduct lessons learned review
- Update policies and procedures
- Prepare incident report
- Notify relevant parties as required

6.4 Communication and Notification
• Internal notification within 2 hours of confirmed incident
• Customer notification per applicable regulations (CCPA, etc.)
• Regulatory notification as required by law
• Vendor notification for third-party service impacts

---

7. VULNERABILITY MANAGEMENT

7.1 Vulnerability Assessment
• Automated dependency scanning via GitHub Dependabot
• Regular security assessments of critical systems
• Third-party security testing annually or after major changes
• Continuous monitoring for new vulnerabilities

7.2 Patch Management
• Critical security patches applied within 72 hours
• High-priority patches applied within 7 days
• Regular patches applied within 30 days
• Emergency patching procedures for zero-day vulnerabilities

7.3 Secure Development
• Security-by-design principles in development lifecycle
• Secure coding standards and practices

• Security testing integrated into development process
• Code review requirements for all changes

---

8. EMPLOYEE AND CONTRACTOR SECURITY REQUIREMENTS

8.1 Security Awareness Training
• Annual security awareness training for all personnel
• Specialized training for developers and administrators
• Phishing awareness and testing program
• Security policy acknowledgment required

8.2 Background Checks
• Background verification for employees with access to sensitive data
• Reference checks for all personnel
• Ongoing verification for contractors and third parties

8.3 Acceptable Use
• Approved use of company systems and data
• Prohibition of unauthorized software installation
• Personal use limitations and guidelines
• Social media and public communication guidelines

8.4 Bring Your Own Device (BYOD)
• Mobile device management (MDM) for company data access
• Encryption requirements for personal devices
• Remote wipe capability for lost or stolen devices
• Separation of personal and business data

---

9. THIRD-PARTY VENDOR MANAGEMENT

9.1 Vendor Security Assessment
All critical vendors undergo security assessment including:
• **Plaid (Identity/Financial Verification):** SOC 2 Type II compliant, bank-level security
• **Supabase (Database/Backend):** SOC 2 compliant, AES-256 encryption, row-level security
• **Cloudflare (CDN/Security):** Enterprise-grade DDoS protection, WAF, TLS termination
• **GitHub (Code Repository):** Automated security scanning, access controls

9.2 Vendor Requirements
• SOC 2 Type II compliance preferred for critical vendors

• Contractual security requirements and liability provisions
• Regular security assessments and compliance verification
• Incident notification requirements
• Data processing agreements (DPA) where applicable

9.3 Vendor Monitoring
• Ongoing monitoring of vendor security posture
• Regular review of vendor security reports
• Incident response coordination with vendors
• Annual vendor security review

---

10. BUSINESS CONTINUITY AND DISASTER RECOVERY

10.1 Business Impact Analysis
• Critical business functions identified and prioritized
• Recovery time objectives (RTO) and recovery point objectives (RPO) defined
• Dependencies on third-party services documented
• Alternative processing capabilities identified

10.2 Backup and Recovery
• **Database Backups:** Automated daily backups via Supabase with point-in-time recovery
• **Application Code:** Version control and automated deployment pipelines
• **Configuration Data:** Infrastructure as code with version control
• **Recovery Testing:** Quarterly backup restoration testing

10.3 Incident Response Integration
• Security incident response integrated with business continuity plans
• Communication procedures during outages
• Vendor escalation procedures
• Customer communication templates

---

11. COMPLIANCE AND LEGAL REQUIREMENTS

11.1 Regulatory Compliance
• **SOC 2 Type II:** Alignment with SOC 2 principles for service organizations
• **California Consumer Privacy Act (CCPA):** Privacy rights for California residents
• **State Privacy Laws:** Compliance with applicable state privacy regulations
• **Financial Data Protection:** Compliance with financial data protection requirements

11.2 Contractual Requirements
• Customer data processing agreements
• Vendor security requirements compliance
• Insurance requirements for cyber liability
• Indemnification and liability provisions

11.3 Audit and Assessment
• Annual security assessment by qualified third party
• Internal security reviews quarterly
• Compliance audits as required by regulations
• Documentation retention for audit purposes

---

12. POLICY GOVERNANCE

12.1 Policy Review and Updates
• **Annual Review:** Complete policy review and update cycle
• **Triggered Reviews:** Updates based on incidents, technology changes, or regulatory changes
• **Approval Process:** CEO approval required for all policy changes
• **Communication:** Policy changes communicated to all affected personnel

12.2 Policy Enforcement
• Regular monitoring and assessment of policy compliance
• Non-compliance reporting and investigation procedures
• Disciplinary actions for policy violations
• Continuous improvement based on lessons learned

12.3 Training and Awareness
• Policy acknowledgment required for all personnel
• Regular training updates on policy changes
• Security awareness programs aligned with policy requirements
• Performance metrics for policy compliance

---

13. CONTACT INFORMATION

Policy Owner: Amanda Bradford, CEO
Email: amanda@hatchlabs.com
Business Address: 701 Tillery Street, Suite 12, Austin TX 78702

Emergency Security Contact: amanda@hatchlabs.com
Incident Reporting: amanda@hatchlabs.com

---

14. DOCUMENT CONTROL

Document History:
• Version 1.0 - March 6, 2026 - Initial policy creation

Related Documents:
• Privacy Policy
• Acceptable Use Policy
• Incident Response Procedures
• Data Classification Guidelines

Next Scheduled Review: March 6, 2027

This document contains confidential and proprietary information of Hatch Labs Holdings LLC. Unauthorized distribution is prohibited.