Thrive in3, LLC

Comprehensive Information Security and Data Privacy Policies

Company: Thrive in3, LLC
Revision Date: [6-28-2025]
Supervisor: Kate Matthew

1. Information Security Policy

Purpose

This policy establishes the overall security governance framework for Thrive in3, LLC to protect sensitive data throughout its lifecycle and ensure compliance with applicable regulations including FERPA, COPPA, GDPR, and other privacy laws.

Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to Thrive in3, LLC's information systems and data, including educational records protected under FERPA and children's personal information subject to COPPA requirements.

Policy Statement

Thrive in3, LLC is committed to protecting the confidentiality, integrity, and availability of all information assets, with special attention to educational records under FERPA and children's personal information under COPPA. All personnel must comply with security requirements and report security incidents immediately

Responsibilities

The following defines the roles and responsibilities under this policy.

Supervisor: Overall accountability for information security program
IT Contractor: Implementation and maintenance of technical security controls
All Employees and Consultants: Adherence to security policies and reporting of security incidents
Management: Ensuring adequate resources and support for security initiatives

Data Classification

The following defines the classification and handling for data under this policy.

Public: Information that can be freely shared
Internal: Information restricted to organization personnel
Confidential: Sensitive information requiring special protection

Restricted: Highly sensitive information with strict access controls
FERPA Protected: Educational records requiring compliance with FERPA regulations

Security Controls

The following security controls shall be implemented and maintained pursuant to this policy.

- Access controls must be implemented based on principle of least privilege
- Data encryption required for sensitive information in transit and at rest
- Regular security assessments and audits must be conducted
- Incident response procedures must be followed for all security events

Review and Updates

This policy will be reviewed annually and updated as necessary to address new threats and regulatory requirements.

2. Access Control Policy

Purpose

To ensure that access to information systems and data is appropriately controlled and monitored.

Scope

All information systems, applications, and data repositories within Thrive in3, LLC, including systems containing FERPA-protected educational records and COPPA-regulated children's information.

Access Control Requirements

User Account Management

- Unique user IDs must be assigned to each individual
- Shared accounts are prohibited except for approved system accounts
- User accounts must be created through formal approval process
- Default passwords must be changed immediately upon account creation

Role-Based Access Control

- Access rights assigned based on job responsibilities and business need
- Principle of least privilege must be applied
- Regular access reviews conducted quarterly
- Segregation of duties implemented for critical functions

- FERPA Compliance: Access to educational records limited to authorized personnel with legitimate educational interest
- COPPA Compliance: Enhanced access controls for children's personal information with additional approval requirements

Access Termination

- Access must be revoked immediately upon employment or consultant termination or at the end of the relevant contractor agreement
- Manager must ensure termination of account access within 24 hours of termination or the end of the relevant agreement
- Access reviews triggered by role changes or transfers

Multi-Factor Authentication

- Required for all remote access and privileged accounts
- Must be implemented for access to sensitive systems and data

Monitoring and Compliance

- Access logs must be monitored and reviewed monthly
- Failed login attempts tracked and investigated

3. Network Security Policy

Purpose

To protect the organization's network infrastructure and ensure secure communication channels, with special considerations for FERPA and COPPA protected data transmission.

Scope

All network devices, connections, and communications within Thrive in3, LLC's environment, including networks transmitting FERPA-protected educational records and COPPA-regulated children's information.

Network Security Requirements

Firewall Management

- Firewalls required at all network perimeters
- Default deny-all policy with specific allow rules
- Firewall rules reviewed and updated quarterly
- Change management process required for all firewall modifications

Network Segmentation

- Sensitive systems isolated through network segmentation
- DMZ implemented for internet-facing services
- Internal network zones based on security requirements
- VLANs used to separate different types of traffic

Password and Authentication Standards

- Default passwords prohibited on all network devices
- Strong password requirements enforced (minimum 10 characters)
- Regular password changes required for network device accounts

Wireless Network Security

- WPA3 encryption required for all wireless networks
- Regular wireless security assessments conducted

Remote Access Security

- VPN required for all remote network access
- Multi-factor authentication required for VPN access

Monitoring and Maintenance

- Network traffic monitored for suspicious activity
- Intrusion detection/prevention systems deployed
- Regular vulnerability scans of network infrastructure
- Network device configurations backed up regularly

4. Vulnerability Management Policy

Purpose

To establish systematic procedures for identifying, assessing, and remediating security vulnerabilities.

Scope

All information systems, applications, and network infrastructure owned or operated by Thrive in3, LLC, with enhanced protections for systems processing FERPA educational records and COPPA-regulated children's data.

Vulnerability Management Process

Regular Security Testing

- Vulnerability scans conducted monthly on all systems
- External vulnerability assessments performed at reasonable intervals
- Web application security testing conducted before deployment
- Database security assessments performed annually

Penetration Testing

- Annual penetration testing by qualified third parties
- Testing scope includes network, application, and physical security
- Results reviewed by senior management
- Remediation plans developed for all identified vulnerabilities

File Integrity Monitoring

- Critical system files monitored for unauthorized changes
- Log analysis performed daily for integrity violations
- Alerts generated for unauthorized file modifications
- Baseline configurations maintained for all systems

Anti-Virus and Anti-Malware

- Current anti-virus software deployed on all endpoints
- Real-time scanning enabled with automatic updates
- Full system scans performed at reasonable intervals
- Quarantine procedures for detected malware

Remediation Requirements

- Critical vulnerabilities patched as soon as practicable but in not more than five (3) business days
- High-risk vulnerabilities addressed within thirty (30) days
- Medium-risk vulnerabilities remediated within ninety (90) days
- Compensating controls implemented when patching not feasible

Documentation and Reporting

- Vulnerability scan results documented and tracked
- Periodic vulnerability reports provided to management at commercially reasonable intervals
- Remediation progress tracked

5. Data Retention and Disposal Policy

Purpose

To establish guidelines for the retention, storage, and secure disposal of organizational data, including compliance with FERPA educational record retention requirements and COPPA data minimization principles.

Scope

All data created, received, or maintained by Thrive in3, LLC in any format, including FERPA-protected educational records and COPPA-regulated children's personal information.

Data Retention Requirements

Retention Schedules

- Financial records: 7 years
- Employee records: 5 years after termination
- Customer data: As required by contract or regulation (generally no greater than sixty days after termination of agreement)
- Email communications: 3 years
- System logs: 1 year minimum
- FERPA Educational Records: Does not general alter length of retention as data provided to or returned to institution to which FERPA applies; must adhere to terms of contract
- COPPA Children's Data: Retained only as long as reasonably necessary for the purpose collected; deleted when child reaches 13 or upon parent request

Storage Limitations

- Data stored only for legitimate business purposes
- Regular reviews to identify unnecessary data for disposal
- Data minimization principles applied to all collection
- Cloud storage subject to same retention requirements

Secure Disposal Procedures

Electronic Data Disposal

- Multi-pass overwriting required for sensitive data
- Cryptographic erasure acceptable for encrypted data
- Hard drives physically destroyed when replacement occurs
- Certificate of destruction should be completed; adhere to reporting requirements of individual agreements.

- Compliant data deidentification and anonymization may be considered proposal disposal; must be confirmed per the provisions of the applicable agreement.

Physical Document Disposal

- Confidential documents shredded using cross-cut shredders
- Secure disposal containers used for sensitive materials
- Disposal activities logged and monitored
- Third-party disposal services must be certified

Compliance and Monitoring

- Annual review of retention schedules
- Data disposal activities documented and audited
- Legal holds override standard retention schedules; Holds instituted by outside counsel in consultation with management

6. Privacy Policy

Purpose

To inform individuals about how their personal information is collected, used, and protected by Thrive in3, LLC, with specific provisions for FERPA educational records and COPPA compliance for children under 13. A more extensive, external facing privacy policy will be posted on Thrive in3, LLC's website and updated as required.

Information We Collect

We collect or may collect the following types of personal information:

- Contact information (name, email, phone number, address)
- Account information (username, password, preferences)
- Transaction data (purchase history, payment information)
- Usage information (website activity, device information)
- Location data (when explicitly consented to)
- Educational Records (FERPA): Progress reports, lesson plans and other educational information.

How We Use Information

Personal information is used for:

- Providing and improving our services
- Processing transactions and communications
- Marketing and promotional activities (with consent)

- Legal compliance and fraud prevention
- Customer support and service delivery
- Educational Purposes (FERPA): Maintaining educational records, providing educational services, and academic administration

Information Sharing

We may share personal information with:

- Service providers and business partners (under contract)
- Legal authorities when required by law
- Other parties with explicit consent
- Affiliated companies
- FERPA Disclosures: Educational records shared only with school officials with legitimate educational interest, authorized parties for audit purposes, or as required by law

We do not sell personal information to third parties. Educational records and children's information are never sold or used for commercial marketing purposes.

Data Protection Measures

- Encryption of sensitive data in transit and at rest
- Access controls limiting data access to authorized personnel
- Regular security assessments and monitoring
- Secure data centers with physical and logical protections
- Employee training on data privacy and security

Individual Rights

Individuals have the right to:

- Access their personal information
- Correct inaccurate information
- Delete personal information (where legally permissible)
- Object to processing or withdraw consent
- Data portability (receive data in structured format)
- FERPA Rights: Students and parents have the right to inspect educational records, request corrections, and control disclosure of information

7. Data Breach Response Policy

Purpose

To establish procedures for responding to data security incidents and breaches of personal information, including specific requirements for FERPA educational records and COPPA-protected children's information.

Scope

All data security incidents involving Thrive in3, LLC's systems, data, or personnel, with enhanced procedures for incidents involving FERPA educational records or COPPA-protected children's information.

Incident Response Team

- Incident Commander: Kate Matthew, Founder & Member
- IT Security Representative: Contracted Consultant
- Legal Counsel: Outside Privacy Counsel
- Privacy Officer: Kate Matthew, Founder & Member
- Communications Lead: Kate Matthew, Founder & Member

Incident Classification

- Level 1: Minor incidents with no data exposure
- Level 2: Potential data exposure requiring investigation
- Level 3: Confirmed data breach requiring notification

Response Procedures

Immediate Response (0-24 hours)

1. Identify and contain the incident
2. Assess scope and severity of breach
3. Activate incident response team
4. Document all actions taken
5. Preserve evidence for investigation

Investigation Phase (24-72 hours)

1. Conduct detailed forensic analysis
2. Determine root cause of incident
3. Assess data compromised and individuals affected
4. Evaluate risk to affected individuals
5. Develop remediation plan

Notification Requirements

- Regulatory Authorities: As required
- Affected Individuals: Without undue delay
- Law Enforcement: When criminal activity suspected
- Insurance Provider: As required by policy terms
- FERPA Incidents: Work with education partners on Department of Education notification for significant breaches of educational records
- COPPA Incidents: FTC notification and enhanced parental notification for children's data breaches

Communication Templates

Pre-approved templates maintained for:

- Regulatory notifications
- Individual breach notifications
- Media statements
- Employee communications
- Customer service responses

Post-Incident Activities

- Lessons learned review conducted
- Policies and procedures updated
- Additional training provided if needed
- Monitoring enhanced for similar incidents

8. Employee Training Policy

Purpose

To ensure all personnel receive appropriate privacy and security awareness training, including specific requirements for FERPA and COPPA compliance.

Scope

All employees, contractors, and temporary workers with access to organizational systems or data.

Training Requirements

New Employee Orientation

- Security and privacy awareness training within first week
- Role-specific training for positions with data access
- Acknowledgment of policies and procedures required
- Completion documented in employee file

Ongoing Training

- Annual security awareness training for all personnel
- Quarterly updates on new threats and procedures
- Specialized training for IT and security staff
- Incident-specific training following security events

Training Topics

- Password security and multi-factor authentication
- Email security and phishing awareness
- Data classification and handling procedures
- Privacy rights and obligations
- Incident reporting procedures
- Physical security measures
- Remote work security practices
- FERPA Training: Educational record privacy requirements, legitimate educational interest, and disclosure procedures
- COPPA Training: Children's privacy protection, parental consent requirements, and data minimization principles

Training Delivery Methods

- Interactive online modules
- In-person workshops and seminars

- Security awareness newsletters

Documentation and Compliance

- Training completion tracked
- Non-compliance escalated to management

Training Effectiveness

- Knowledge assessments following training
- Regular security awareness surveys
- Incident rates monitored as training effectiveness metric

9. Vendor Management Policy

Purpose

To ensure third-party vendors adequately protect personal data and maintain appropriate security standards, with enhanced requirements for vendors processing FERPA educational records or COPPA-regulated children's information.

Scope

All vendors, suppliers, and service providers that process personal data on behalf of Thrive in3, LLC, including those with access to FERPA educational records or COPPA-protected children's information.

Vendor Classification

- High Risk: Vendors with access to sensitive personal data
- Medium Risk: Vendors with limited data access
- Low Risk: Vendors with no access to personal data

Due Diligence Requirements

Pre-Engagement Assessment

- Security questionnaire completion
- Financial stability review
- Reference checks with existing customers
- Certification and compliance verification
- Risk assessment based on data access level

Security Requirements

- Data encryption in transit and at rest
- Access controls and authentication measures
- Incident response and breach notification procedures
- Employee background checks and training
- Regular security assessments and audits

Contract Provisions

All vendor contracts must include:

- Data processing agreement (DPA)
- Security requirements and standards
- Breach notification obligations
- Right to audit and inspect
- Data return or destruction upon termination
- Limitation of liability and indemnification
- Subprocessor approval requirements

Ongoing Monitoring

- Annual security assessments
- Quarterly business reviews including security topics
- Continuous monitoring of vendor security posture
- Regular contract reviews and updates
- Vendor performance scorecards

Incident Management

- Vendor incident reporting requirements
- Joint incident response procedures
- Communication protocols during incidents
- Documentation and lessons learned

Contract Termination

- Data return or secure destruction
- Access revocation procedures
- Final security assessment
- Transition planning for service continuity

10. Data Subject Rights Policy

Purpose

To establish procedures for handling individual requests regarding their personal data rights.

Scope

All requests from data subjects regarding their personal information held by Thrive in3, LLC or one of its subcontractors.

Individual Rights Under GDPR/Applicable Privacy Laws

- Right of Access: Obtain confirmation and copy of personal data
- Right to Rectification: Correct inaccurate personal data
- Right to Erasure: Delete personal data under certain conditions
- Right to Restrict Processing: Limit how personal data is used
- Right to Data Portability: Receive personal data in structured format

Request Handling Procedures

Request Receipt and Validation

- Requests accepted via email or mail
- Identity verification required before processing
- Requests logged in data subject rights management system
- Acknowledgment sent within five (5) business days

Processing Timeline

- Standard response time: thirty (30) days
- Complex requests: Up to ninety (90) days (with notification)
- Urgent requests (data portability): twenty (20) days
- Free of charge unless requests are excessive or require significant resource allocation

Response Procedures

- Legal review for complex or unusual requests
- Third-party notification when applicable
- Response provided in accessible format (generally csv)
- Documentation of all actions taken

Request Types and Procedures

Access Requests

- Provide copy of personal data held
- Explain processing purposes and legal basis
- Identify recipients of shared data
- Specify retention periods
- Inform of individual rights

Correction Requests

- Verify accuracy of claimed corrections
- Update data in all relevant systems
- Notify third parties of corrections when required
- Provide confirmation of changes made

Deletion Requests

- Assess legal basis for retention
- Identify all systems containing the data
- Perform secure deletion procedures
- Notify third parties when applicable
- Document deletion completion

Escalation and Appeals

- Complex requests escalated to privacy officer
- Legal consultation for disputed requests
- Appeals process for denied requests
- Regulatory authority complaint procedures

Training and Awareness

- Regular training for staff handling requests
- Clear procedures and decision trees
- Regular review of response quality
- Continuous improvement based on feedback

Policy Version: 1.0
Next Review Date: 6-28-2026
Document Owner: Management
Approved By: Kate Matthew, Founder & Member