FinalForms Information Security Policy

1. Purpose

The purpose of this Information Security Policy is to protect the confidentiality, integrity, and availability of FinalForms' data, systems, and networks. This policy establishes security requirements to ensure the safe handling of sensitive information, including student data, while supporting operational activities and complying with legal and regulatory obligations.

2. Scope

This policy applies to all employees, contractors, vendors, and partners of FinalForms who have access to FinalForms' information systems, including but not limited to:

- Internal systems such as registration platforms.
- External applications and third-party services.
- Data stored, processed, or transmitted by the company.

3. Roles and Responsibilities

- **Chief Security Officer (CSO)**: Responsible for implementing and overseeing security programs, policies, and incident response.
- **Chief Technology Officer (CTO)**: Ensures that technical security controls are in place to safeguard systems.
- **All Employees and Contractors**: Must comply with security policies and report any incidents or suspicious activities.
- **External Vendors**: Must adhere to FinalForms' security standards and undergo regular security assessments.

4. Information Security Principles

4.1 Confidentiality

- Only authorized users may access sensitive information such as student medical data, parent contact details, and compliance records.
- Access controls, role-based permissions, and encryption must be applied to ensure that unauthorized users do not access sensitive information.

4.2 Integrity

- Systems and data must be protected against unauthorized modification or destruction.
- Controls must be implemented to ensure the accuracy, consistency, and reliability of data through automated checks and validation processes.

4.3 Availability

- Systems must be available as specified in the Service Level Agreement (SLA) to avoid disruption to critical services, including student registration and emergency data access.
- Backup and disaster recovery mechanisms must be in place to ensure that critical data is recoverable in case of an incident.

5. Data Protection and Privacy

- **Data Encryption**: All sensitive data must be encrypted both at rest and in transit using strong encryption algorithms.
- **Access Controls**: All systems will employ multi-factor authentication (MFA), strong password policies, and regular access reviews to minimize risk.
- **Data Retention and Deletion**: Data should be retained only as long as required for operational purposes or as required by law. Outdated or unnecessary data must be securely deleted.
- **Third-Party Data Protection**: All third-party vendors handling sensitive data must adhere to the same security standards and undergo regular security reviews.

6. Risk Management and Incident Response

- **Risk Management**: Regular risk assessments must be conducted to identify, evaluate, and mitigate potential security vulnerabilities or threats. This includes reviews of physical, network, application, and personnel security risks.
- **Incident Response Plan**: In the event of a security breach, including data breaches, unauthorized access, or ransomware attacks, the CSO will coordinate the response. The incident response plan includes:
    - Immediate containment and mitigation.
    - Notification of affected stakeholders.
    - Root cause analysis and remediation.
    - Communication with legal and regulatory authorities, as required.

7. Training and Awareness

- All employees, contractors, and partners must receive regular training on security policies, data privacy, and best practices, such as phishing awareness and secure data handling.
- New hires must undergo mandatory security training during their onboarding process.

8. Monitoring and Audits

- **Monitoring**: All access to FinalForms systems and data must be logged and regularly monitored for suspicious activity.
- **Audits**: Regular internal and third-party security audits will be conducted to ensure compliance with this policy and identify areas for improvement.
- **Vulnerability Testing**: Regular penetration testing, vulnerability scans, and security assessments will be conducted to validate system security.

9. Compliance

FinalForms will comply with all applicable legal, regulatory, and contractual obligations, including FERPA (Family Educational Rights and Privacy Act), COPPA (Children's Online Privacy Protection Act), and any state-level student data privacy laws.

10. Policy Violations

Violations of this Information Security Policy will result in disciplinary actions, including termination of employment or contractual agreements, and may lead to legal actions where necessary.

11. Review and Maintenance

This policy will be reviewed and updated annually or as needed to ensure alignment with changes in technology, business needs, and regulatory requirements.

Approval

This policy is approved by:

- **Clay Burnett, CEO**
- **Griffith Chaffee, Chief Security Officer (CSO)**
- **Macklin Chaffee, Chief Technology Officer (CTO)**