**Appendix D: Cyber Risk Management Requirements for IT and Data Processing Suppliers**

**Cybersecurity Requirements and Evaluation Notice**

**Instructions: This section outlines FAME's cybersecurity expectations for bidders and recommended software platforms. Detailed documentation will be required only from finalist bidders during the presentation and alignment phases. Initial proposals should address these requirements at a high level to demonstrate understanding and capability.**

**CYBERSECURITY EVALUATION FRAMEWORK**

**What We Will Evaluate:**

**FAME will assess bidders on two critical dimensions:**

1. **Your organization's cybersecurity maturity as our trusted implementation partner**
2. **The security posture of platforms you recommend for our technology modernization**

**PROPOSAL RESPONSE REQUIREMENTS**

**For Proposal Submission:**

**Provide a brief narrative addressing:**

1. Security Philosophy: How cybersecurity is integrated into your methodology and platform recommendations
2. Organizational Qualifications: Summary of your security certifications, capabilities, and relevant experience
3. Platform Security Approach: High-level description of how you evaluate and ensure platform security
4. Risk Management: How you identify, assess, and mitigate cybersecurity risks during design and implementation
5. Compliance Experience: Examples of similar projects in regulated environments
6. Note exceptions in the ability of recommended platforms to meet listed security standards.

**SECTION 1: BIDDER ORGANIZATION SECURITY REQUIREMENTS**

**1.1 Baseline Security Expectations**

**In your proposal, confirm that your organization maintains:**

* Documented cybersecurity program with annual reviews and testing
* Third-party security validation (SOC 2 Type II, ISO 27001, or equivalent)
* Cyber liability insurance with minimum $5M coverage
* Incident response capability with client notification protocols
* Secure development practices for custom code development
* Data encryption standards for data at rest and in transit
* Multi-factor authentication for all employees and client system access

**1.2 Data Migration Security Capabilities**

**Confirm your organization has:**

* Proven data migration methodology for regulated environments
* Experience with financial services and educational data (FERPA, GLBA compliance)
* Segregated migration environments with enhanced monitoring
* Data masking/synthetic data capabilities for testing
* Secure data destruction procedures with certification
* Real-time migration monitoring and rollback capabilities

**1.3 What Finalists Will Provide**

**Selected finalists will be required to provide detailed evidence, including:**

* Current third-party security validation (SOC 2 Type II report, ISO 27001, or equivalent)
* Data migration security methodology documentation
* Incident response plan and recent testing results
* Insurance certificates and coverage details

**SECTION 2: RECOMMENDED PLATFORM SECURITY REQUIREMENTS**

**2.1 Platform Security Standards**

**For each software platform you recommend, confirm it meets:**

* SOC 2 Type II compliance (or equivalent security framework)
* Enterprise-grade encryption for data at rest and in transit
* Role-based access controls with SSO/SAML integration
* Comprehensive audit logging with retention and monitoring
* Regular penetration testing and vulnerability assessments
* Data portability and deletion capabilities for vendor independence
* Incident response and business continuity plans

**2.2 Shared Responsibility Model**

**For cloud-based platforms, demonstrate understanding of:**

* Well-Architected Framework implementation guidelines
* Clear delineation of vendor vs. client security responsibilities
* FAME's obligations for configuration, access management, and monitoring
* Integration requirements with FAME's identity and security systems
* Compliance reporting capabilities for regulatory requirements
* Data residency and sovereignty controls

**2.3 What Finalists Will Provide**

**Selected finalists will be required to provide:**

* Security assessment summary for each recommended platform
* Shared responsibility models for all cloud services
* Platform vendor security documentation and certifications
* Risk assessment identifying any security gaps and mitigation strategies
* Integration architecture showing security controls and data flows

**SECTION 3: AI AND EMERGING TECHNOLOGY GOVERNANCE**

**3.1 AI Security Requirements**

**If your solution includes AI/ML components, confirm:**

* Data privacy controls preventing client data from training models
* AI governance policies for bias, fairness, and explainability
* Model security including adversarial attack protection
* Transparency in AI decision-making processes
* Human oversight mechanisms for AI-generated outputs

**SECTION 4: REGULATORY AND COMPLIANCE CONSIDERATIONS**

**4.1 Compliance Framework**

**Demonstrate understanding of FAME's regulatory environment:**

* FERPA compliance for student data protection
* Financial services regulatory requirements for 529 plan, loan and insurance data, reporting, etc.
* State government public records requirements and FOAA considerations

**4.2 What Finalists Will Provide**

**Selected finalists will be required to provide:**

* Detailed compliance mapping for recommended solutions
* Data classification, handling and discovery procedures and capabilities
* Regulatory reporting and audit trail capabilities
* Privacy impact assessment for proposed architecture

**FINALIST EVALUATION PROCESS**

**Detailed Security Review**

To include additional data sharing regarding cybersecurity capabilities and controls.

May include cybersecurity focused interview

**Decision Criteria**

* + Security evaluation may result in bidder disqualification
  + Security evaluation may result in disqualification of recommended platforms

**QUESTIONS AND CLARIFICATIONS**

**For questions regarding cybersecurity requirements, please submit through the standard RFP question process. Common questions will be addressed in the consolidated Q&A document.**

Note: FAME reserves the right to conduct additional security due diligence on the selected vendor, including ongoing security monitoring requirements throughout the engagement.