

Application Development Standards for In-House Applications

Student Affairs Information Technology (SAIT)

Version 1.1 – February 9, 2026

1. Purpose and Scope

1.1 Purpose

This document defines the technical, operational, and security standards for applications developed and supported by Student Affairs Information Technology (SAIT). These standards ensure that internally developed applications are secure, maintainable, scalable, and aligned with Virginia Tech policies and institutional technology requirements.

1.2 SAIT Development Team Role

The SAIT Development Team provides software engineering and application development services **exclusively** for Student Affairs departments.

1.3 Required Collaboration

Student Affairs departments must engage SAIT from **initial planning through implementation and deployment**.

Applications developed without SAIT involvement from project inception **will not be hosted, supported, or maintained** by SAIT.

1.4 Third-Party Vendors

When a department contracts with a third-party vendor for application development, the vendor is solely responsible for hosting, maintenance, and ongoing support unless otherwise documented and approved in writing by SAIT.

2. Application Size and Scope

2.1 Supported Application Size

SAIT focuses on the development and support of **small to mid-size applications**.

A small to mid-size application is defined as one that:

- Requires **fewer than 300 development hours** to reach a Minimum Viable Product (MVP), and
- Supports **fewer than 5,000 active daily users**

Projects exceeding these thresholds must be evaluated for:

- Commercial or vendor-supported solutions, or
- Enterprise IT platforms supported outside of SAIT

3. Pre-Development Assessment

Before a project is approved, the following must be reviewed and documented:

- **Duplication:** Whether an existing Virginia Tech system already meets the requirement
- **Buy vs. Build:** Whether a commercial solution is more sustainable than custom development
- **Maintenance:** Availability of a long-term support and maintenance plan
- **Platform Fit:** Suitability of the Microsoft Power Platform (low-code/no-code)
- **Ownership:** Identification of a departmental owner responsible for approvals, enhancements, and change requests

4. Technical Architecture and Standards

4.1 Standard Application Architecture

SAIT-supported applications use a standardized **LAMP-based architecture**:

Component	Standard
Operating System	Linux
Web Server	Apache

Database	MariaDB
Backend Language	PHP (currently supported versions only)
Framework	CodeIgniter
Frontend	JavaScript with Vue.js

4.2 Unsupported Technologies

- Document-oriented databases (e.g., MongoDB) are not supported
- **Legacy Exception:** Visual Basic .NET is supported only for explicitly approved legacy systems.

4.3 Coding and Secure Development Standards

All applications must follow industry best practices and secure coding standards, including:

- Input validation and sanitization
- Authentication and authorization controls
- Encryption of sensitive data
- Protection against common vulnerabilities (e.g., OWASP Top 10)
- Regular peer code reviews and security testing

All development must comply with applicable university policies and regulatory requirements.

4.4 Version Control

- All projects must use the SAIT-approved version control system
- Repository access is restricted to authorized users and secured virtual machines
- All repositories must include a `.gitignore` file
- **Versioning:** Semantic Versioning is required (e.g., v1.0.0)

4.5 Authentication

All applications requiring authentication must implement an **approved Virginia Tech Single Sign-On (SSO)** solution.

5. Security and Compliance

5.1 Authentication and Authorization

- SSO is required for all authenticated applications
- Role-Based Access Control (RBAC) must be implemented
- User sessions must expire after a defined period of inactivity

5.2 Data Protection

- **Encryption at Rest:** Databases must be encrypted
- **Encryption in Transit:** HTTPS is required for all applications
- **Secrets Management:** Credentials and API keys must be stored securely and never committed to source control
- **PII and FERPA Data:**
 - Restricted data may exist only in secured production environments
 - Real PII must **never** be used in development or testing environments

5.3 Auditing

- Applications must maintain audit logs appropriate to their risk level
- Audit summary notifications must be provided to application administrators **at least once per semester**

6. Testing, Deployment, and Hosting

6.1 Testing Requirements

- **Backend:** PHPUnit unit tests are required
- **Frontend / End-to-End:** Playwright testing is required

6.2 CI/CD and Deployment

- All deployments must be automated using **GitLab Pipelines**
- Each project requires a one-time server configuration
- All subsequent deployments must be fully automated

6.3 Hosting

All supported applications are hosted on **SAIT-managed infrastructure**.

6.4 Maintenance Expectations

Issue Type	Target Response
Security vulnerabilities	Within 24 hours
Non-security issues	Within 72 hours
Server patching	Monthly or immediately for critical CVEs

7. Documentation Requirements

Each project repository must include a /documentation directory containing:

- Entity Relationship Diagrams (ERDs) – MySQL Workbench
- Process flow diagrams – Visio or PDF
- Client requirements documentation
- README with local development setup instructions

Appendix A: Low-Code / No-Code Standards (Microsoft Power Platform)

A.1 Scope

The Microsoft Power Platform may be used for:

- Power Automate (workflow automation)
- Power Apps (application development)
- Power BI (reporting and analytics)

A.2 Governance and Review

- Requests must be submitted through the SAIT Help Desk
- SAIT determines the appropriate solution approach

- **Power BI projects require Assessment, Evaluation, and Data Strategy (AEDS) approval prior to development**

A.3 Ownership and Service Accounts

- Only solutions owned by the **SAIT Service Account** are officially supported
- Solutions built under personal accounts are not supported
- Departmental solutions must be transferred to the SAIT Service Account for support eligibility

A.4 Environment Standards

- **Development:** Build, testing, and business validation only
- **Production:** End-user solutions only; no direct development permitted
- Solution-based development is required
- Managed solutions are required in Production

A.5 Platform-Specific Standards

Power Apps

- Must be responsive and accessible
- Only approved data sources (Dataverse, SQL, SharePoint)
- Must meet organizational accessibility standards

Power Automate

- Premium connectors must run in Production
- Hard-coded credentials are prohibited
- Error handling and notifications (Teams or email) are required

Power BI

- PBIX files must be version-controlled in SharePoint or OneDrive
- AEDS approval is required prior to report publication

A.6 Maintenance

SAIT monitors platform performance and licensing usage. Unsupported or inactive solutions may be disabled to maintain security and stability.

8. Revision Policy

Student Affairs IT may revise this document as operational needs require, with or without prior notice.