

Organizational Application Management Standard

Purpose

This standard outlines the procedures and best practices for managing organizational applications, ensuring security, compliance, and efficiency across all departments within Student Affairs. It applies to both vendor-supported and homegrown applications managed by departmental administrators.

1. Approved Software and Approval Process

Objective

Ensure all software used within Student Affairs is compliant with university standards, procured through approved channels, and adheres to security, privacy, and accessibility requirements.

1. Approval Process for Regular Software:

- a. All software purchases must be reviewed and approved by Virginia Tech's [IT Procurement](#) department to ensure compatibility with institutional policies and existing systems.
- b. This includes verification of licensing agreements, vendor compliance with data protection standards, and alignment with accessibility guidelines.

2. Low-Cost/Low-Risk Software Category:

- a. For software deemed low-cost (under a predetermined financial threshold) and low risk (minimal security or privacy implications), departments may follow an [expedited approval process](#).

- b. Even for low-risk software, departments must complete a basic compliance checklist provided by IT Procurement to ensure no data security or accessibility issues are overlooked.

3. Procurement Documentation:

- a. All application purchases should be documented, including licensing terms, vendor agreements, and usage guidelines. Departments must retain procurement records in line with Virginia Tech's policies on record-keeping and auditing.

4. Ongoing Compliance:

- a. Software use must adhere to evolving institutional policies, with periodic reviews to ensure ongoing compliance with Virginia Tech's standards on security, data privacy, and accessibility.

For further guidance on IT procurement procedures and requirements, refer to the Virginia Tech IT Procurement page [here](#).

2. Application Management

Objective

Establish clear responsibilities and expectations for application administrators to ensure the secure, efficient, and effective management of critical organizational applications.

Application Administrator Role

All critical SA applications must have a designated application administrator who assumes primary responsibility for their management. Application administrators should have advanced knowledge of departmental business processes and the applications they oversee, including their functionalities, configurations, and integration points with other systems.

Key Responsibilities of Application Administrators

1. Access Management

- Review and approve access requests based on job roles and organizational needs.
- Maintain updated records of user access levels.
- Conduct regular access audits and ensure timely offboarding of users.

2. Application Knowledge and Training

- Acquire and maintain advanced knowledge of application features, updates, and best practices.
- Provide onboarding and training sessions for new users, ensuring compliance with relevant policies (e.g., FERPA, PII, ePHI).
- Act as a subject matter expert for departmental staff and stakeholders.

3. Monitoring and Maintenance

- Oversee daily application operations, ensuring uptime and performance.
- Monitor application logs for anomalies and report incidents to the appropriate teams.
- Schedule and apply application updates or patches in collaboration with vendors or the IT team.

4. Compliance and Security

- Ensure applications comply with university standards for security, data privacy, and accessibility.
- Perform periodic reviews to confirm adherence to compliance requirements.
- Collaborate with SAIT staff to address vulnerabilities and enhance safeguards.

5. Data Management

- Maintain accurate documentation of application configurations, integrations, and workflows.
- Oversee data accuracy and integrity within the application.
- Manage data exports, imports, or migrations as required, adhering to data governance policies.

6. Incident Management

- Act as the primary point of contact for resolving application-related issues.
- Escalate major incidents to IT team, security teams, or vendors as necessary.
- Participate in post-incident reviews and implement corrective actions.

7. Planning and Improvement

- Collaborate with SAIT and departmental leaders on future enhancements or feature requests.
- Provide feedback on application usability and recommend improvements.
- Participate in long-term planning for application upgrades or replacements.

Backup Administrator

To ensure continuity, each critical application must also have a designated backup administrator. This individual should have sufficient knowledge and training to perform key administrative tasks in the primary administrator's absence.

3. Onboarding and Offboarding Workflow

Objective

Ensure controlled access to applications and prevent unauthorized access.

- **Access Management:** Each application must have a designated administrator or coordinator with the authority to manage and assign access levels. These individuals are responsible for reviewing and approving all access requests.
- **Access Requests:** Departmental application users or their supervisors must submit formal access requests through the [application access request form](#), providing a clear justification for the requested access level.
- **Pre-Access Training:** It is strongly recommended that all new users complete the appropriate training based on compliance requirements specified by application administrators (e.g., ePHI, PII, PCI, FERPA) and IT security training (e.g., Securing the Human) before being granted access. Users must provide proof of completed FERPA training if the requested application stores FERPA-related data.
- **Trainee Access:** New users should be initially granted the lowest-level access until they successfully complete formal application onboarding and training provided by departmental managers or application administrators. Documentation of completed training and user access level granted should be kept by the Application Manager.
- **Offboarding:** User access must be revoked immediately upon separation from the department or institution. Departmental Access Provisioning Network (DAPN) members must complete a [offboarding request form](#) for departing employees.

4. Access Control Enhancement

Objective

Limit access based on job roles to minimize security risks.

Role-Based Access: Application access levels should be clearly defined. Depending on the application, specific roles may include:

- **Contributor:** Users who can add or upload data or content but cannot edit or delete it.
- **Editor:** Users who can add and modify content or data and perform quality control but cannot access critical system configurations.
- **User:** General users with view-only access.
- **Super User (Administrator):** Application Administrator responsible for overseeing operations and user management.
- **Backup Administrator:** A designated departmental user to manage the application in the absence of the main administrator.
- **Technical Liaison:** A technical specialist who can handle system-level technical issues and data integration.

5. Access Level Review and Auditing

Objective

Ensure that user access aligns with job responsibilities and organizational needs.

- **Periodic Access Reviews:** Conduct regular interviews and reviews for users with elevated access to confirm their access needs and responsibilities.
- **Audit System Users:** Regularly audit user access and permissions to ensure consistency with departmental requests and approval by the application owner.

6. Data Integration and Automation

Objective

Facilitate seamless data sharing and ensure data consistency across systems.

- **Automated Data Integration:** Implement secure and reliable data integration solutions for applications that transfer data to other university systems (e.g., Banner, Data Lake).
- **Data Mapping and Transformation:** Establish clear rules for data mapping to ensure accurate data representation across all systems.
- **Monitoring and Error Handling:** Implement robust monitoring and error-handling processes to ensure data integrity and reliability.

7. Training and Compliance

Objective

Ensure all users are trained and compliant with organizational and legal standards.

- **Mandatory Training:** Users should complete specific training programs (e.g., FERPA, HIPAA, Securing the Human) to access and manage applications.
 - **FERPA Training:** Required every two years to comply with federal regulations.
 - **IT Security Training:** Annually to promote safe system usage and security awareness.
- **Ongoing Training:** Periodic role-based training should be provided, with training materials available through internal platforms (e.g., Canvas).
- **Access Suspension for Non-Compliance:** Users who fail to maintain current training records may have their access temporarily suspended for applications categorized as [high risk](#) until compliance is demonstrated.

8. Roles and Responsibilities

Objective

Define clear roles and responsibilities to ensure accountability in application management.

- **SAIT Security Analyst:** Responsible for monitoring audit compliance, data integrity, and follow-up on audit forms.
- **Application Administrators:** Conduct audits, manage access permissions, and submit reports.
- **Departmental Leadership:** Ensure compliance with audit procedures and effective offboarding of team members.
- **SAIT Developers:** Handle technical implementation, maintenance of audit forms, and integration with university systems.
- **Vendor:** External party responsible for providing support, maintenance, and updates as agreed. The vendor may collaborate with SAIT and application administrators for specific configurations or technical troubleshooting.

9. Security and Compliance Considerations

Objective

Maintain alignment with organizational security and compliance requirements.

- **Data Privacy and Compliance:** Secure data from audits and the centralized access database to ensure compliance with privacy regulations.
- **Access Control Policies:** Reinforce broader organizational access control policies through regular audits and access reviews.
- **Incident Response:** Outline steps for handling unauthorized access detected during audits.

10. Incident Management and Recovery

Objective

Define a structured process to manage application-related incidents, minimize downtime, and protect data integrity while ensuring swift resolution.

- **Incident Reporting and Escalation:** Application administrators must be promptly informed of all incidents affecting application performance, security, or accessibility.
- **For critical incidents:** Such as data breaches or system outages, the issue must be escalated immediately to the SAIT Security Analyst and departmental leadership.
- **Backup and Recovery:** Critical applications must follow Virginia Tech's data retention and backup policies, with regularly scheduled backups of key data.
- **Post-Incident Review:** For major incidents, application administrators will conduct a post-incident review to identify root causes and implement measures to prevent recurrence. Necessary updates to policies, procedures, or training materials should be made as part of the review process.

11. Application Lifecycle Management

Objective

Provide a structured framework to manage applications effectively from initial implementation to decommissioning, ensuring alignment with organizational goals and compliance requirements.

- **Implementation:**
 - Needs Assessment: Conduct a comprehensive evaluation to justify the development or procurement of new applications.
 - Compliance: Ensure all new applications align with Virginia Tech's IT procurement, security, and accessibility standards.
 - Homegrown Applications: Adhere to coding best practices, maintain version control, and perform thorough security and accessibility reviews prior to deployment.
- Ongoing Maintenance
 - If applicable, schedule and implement regular updates, including vendor patches and internal enhancements, to ensure applications remain secure and functional.
 - Maintain detailed documentation of updates and changes, ensuring consistency across all systems.
 - Conduct periodic evaluations to assess application performance and user satisfaction.
- Monitoring and Support
 - Monitoring tools should be used (by the vendor or the SAIT team) to track application health, user activity, and potential vulnerabilities.
 - Vendor supported critical applications must have a university approved support contract to provide ongoing technical support through a structured helpdesk system to address user issues efficiently.
- Decommissioning
 - Assessment: Regularly evaluate whether the application continues to meet organizational needs or if it should be retired.
 - Data Migration and Archival: Safely migrate critical data to replacement systems or securely archive it following university policies.
 - Communication: Notify stakeholders of decommissioning timelines and alternative solutions well in advance.

- Removal: Ensure all access, licenses, and configurations are removed to fully decommission the system.
- Documentation
 - Maintain a complete lifecycle record for each application, including procurement details, change logs, and decommissioning reports, to support compliance and audit requirements.

12. Continuous Improvement and Review

Objective

Regularly evaluate and improve application management processes.

- **Annual Review:** Conduct an annual assessment to identify areas for improvement based on feedback and audit results.
- **Feedback Mechanism:** Set up a channel for administrators and stakeholders to provide feedback on process effectiveness.
- **Update Schedule:** Ensure updates to this standard are communicated, implemented, and documented.