Application Management Policy

AN ADMINISTRATIVE INFORMATION SECURITY POLICY

PURPOSE

Managing information systems to support business and technical operations requires an organization have a well-defined Software Development Life Cycle (SDLC) framework to manage solutions from inception to disposal. This Application Management Policy establishes policy for a SDLC framework and related software application acquisition and enhancement methodologies that are essential components in the management, development, and delivery of software applications to support business needs and services.

The Application Management Policy must be used for all requests to purchase, acquire or significantly enhance software that will need to be installed on or delivered via the college's networks, or that may perform core academic or administrative functions, so that appropriate technical and support discussions can take place.

SCOPE

This policy applies to all college software, whether purchased, leased, obtained under 'shareware' or 'freeware' arrangements, acquired under suppliers' educational support agreements, or developed in-house.

ROLES & RESPONSIBILITIES

College Leadership: Ensure that the resources they own comply with the guidelines set forth in this policy.

Business Solution Sponsors: Individuals responsible for business operations and must take an active role in the application planning and implementation process. These managers are the individuals with the

authority and responsibility for making decisions essential to application requirements, resources, scheduling, administration and operation.

Information Security Office: The Information Security Office is responsible to ensure compliance with this policy as a component of the College's information security program. In addition, the Information Security Office is responsible to provide training to Business Owners and Users regarding this policy.

ITS Staff: Assists sponsors and owners of the business function to be outsourced with the due diligence required.

Project Manager: Individual responsible for the day-to-day management of a project objectives, tasks, progress, and project team.

System and Application Administrators: Assist Business Solution Sponsors with implementing measures to enforce this policy.

REQUIREMENTS & PRACTICES

Prospective Business Solution Sponsors are strongly encouraged to engage the assistance of Information Technology Services (ITS) as early as possible in project planning (see *IT Governance Policy*). It is recommended that this be considered at project inception and well in advance of establishing budget requirements.

For larger initiatives, a Project Manager should be designated to coordinate associated application, infrastructure, data/information, and security requirements and managed through service design and integrated SDLC frameworks.

All application acquisition and enhancement projects are required to utilize a Secure Software Development Life Cycle (SSDLC) framework that includes the following components:

> **Principles:** Student success, college and technology strategy, revenue generation, and compliance represent several guiding principles that drive decision making under an SSDLC framework. For example, in an effort to reduce the College's legacy and customized application

portfolio as well as ensure effective governance responsibilities, e.g. maintenance of application inventory, the consideration of new or modernizing applications to support business should first emphasize the use of existing solutions.

Information Security: Security assurance activities should be an integral part of all SSDLC activities. Classification and protection of College information assets to ensure confidentiality, integrity and availability should be performed in accordance with the *Data Classification Policy* and *Data Protection Policy*.

Feasibility: Processes and procedures to evaluate and define the best solution approach through research, feasibility studies, analysis of business needs and high-level requirements, resources, capability, capacity, IT investment and risk strategies, alternatives analysis, etc.

Requirements Management: Requirements definition, analysis, refinement, categorization, prioritization, change management, traceability, and documentation procedures and processes based on a software development process model (see *Software Development Policy*).

Design and Development: Specification of functionality, features and operations in detail, prototyping, e.g. screen layout, wireframes, etc., establishment of development environment, and code development and documentation.

Integration, Testing and Verification: Establishment of test environment, test data and quality assurance plan development, testing of developed application for functionality, interoperability, errors, bugs, etc.

Acceptance, Installation and Deployment: Final testing and signoff, deployment into production environment.

Maintenance: Ongoing operational and maintenance requirements, continuous evaluation of application performance.

Evaluation: Review of application performance in production environment, effectiveness and functionality verification, SSDLC process review.

Disposal: Planning and procedures for application retirement or replacement by new solution. Include migration planning, data archival, move or deletion, hardware and software removal, etc.

The recommended approach to solution evaluation and identification is as follows:

1. A robust vetting process should be performed involving the Business Solution Sponsor, Project Manager, ITS, and the Information Security Office to evaluate the following:
    - Determine the impact and capacity of bandwidth on the College network
    - Ensure and maintain enterprise information security
    - Help establish consistent requirements for implementation of the solution
    - Help establish vendor relationship and application procurement vehicles
    - Allow for a centralized review of lessons learned, product experiences, use cases, etc.
    - Determine the impacts to existing environment, capabilities and resources
    - Total cost of ownership
2. Initial emphasis should be given to leveraging available functionality or feature sets within or accompanying applications already deployed at the College, even if these may require business process changes.
3. In situations where existing solutions are unable to satisfy requirements, Commercial-off-the-Shelf (COTS) or Software-as-a-Service (SaaS) solutions should in turn be prioritized over locally developed solutions.
4. When considering leveraging COTS or SaaS solutions, it is important to ensure that solutions chosen can be readily integrated within the current environment to formulate a holistic solution to meet business needs. Evidence of such must be included with required project initiative documentation.

5. If a COTS or SaaS solution has been determined to meet business requirements, departments are required to engage ITS through a Project Request process prior to budget submission.
6. If no third-party solution (i.e. COTS, SaaS, or combination with integration), meets business requirements, next consideration is to be given to custom application development. Sound justification must be provided on why a COTS or SaaS solution alternative is not a viable alternative to custom application development when investing in new, modernizing, or replacing application platform used to support the College mission.

All software applications developed at the College should be created and maintained in accordance with the College's *Software Development Policy*.

All engagements involving contracts or access to Washtenaw Community College information processing facilities, data or assets with third party service providers, including vendors, consultants, and suppliers, shall be in accordance with the College's *Third Party Management Policy*.

COMPLIANCE

This policy is a component of Washtenaw Community College information security program that is intended to comply with the PCI-DSS, FERPA, GLBA, GDPR, HIPAA and other regulations.

EXCEPTIONS

In the event a device or software cannot support this policy compensating controls will be documented and used to mitigate the risk of a breach by a compromised passphrase/password.

The Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the *Request for Policy Exception* form and a copy maintained by the CIO.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Washtenaw Community College reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

DEFINITIONS

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

Software Development Life Cycle (SDLC): A framework that defines the process used by organizations to build an application from its inception to its decommission.

Secure Software Development Life Cycle (SSDLC): A Secure SDLC process ensures that security assurance activities are incorporated throughout the adopted SDLC framework.

REFERENCES

Data Classification Policy

Data Protection Policy

IT Governance Policy

Software Development Policy

Third Party Management Policy

Request for Policy Exception

REVISION HISTORY

Version	Description	Revision Date	Review Date	Approver
1.0	Initial version	10/11/18	-	WJO