Software Development Policy

AN ADMINISTRATIVE INFORMATION SECURITY POLICY

PURPOSE

The purpose of this policy is to establish software development requirements for all applications internally developed to support the mission and business requirements of Washtenaw Community College. Standardization of development and coding techniques is essential to ensuring their maintainability, accessibility and security. These requirements are necessary to protect College resources and preserve the integrity, availability and confidentiality of the College's information assets.

SCOPE

This policy applies to all employees, contractors and consultants involved in the development, modification, maintenance or support of custom software applications or integrations or Software as a Service (SaaS) applications supporting mission and business-related requirements of the College.

ROLES & RESPONSIBILITIES

Business and Functional Stakeholders: Individuals responsible for business operations and must take an active role in the application planning and development 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.

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

Software Developer: Individuals involved in the research, planning, design, programming, integration and testing of computer software or applications.

REQUIREMENTS & PRACTICES

Washtenaw Community College seeks to incorporate a best practice Software Development Life Cycle (SDLC) methodology into software application development processes. SDLC is a standard framework defining processes for analysis, planning, design, development, integration, testing, implementation, operations and maintenance of information systems. Application development requires the use of Agile, an SDLC framework wherever possible.

It is expected that regardless of software development process model in use, appropriate due diligence should be exercised in development, testing and deployment of locally developed software solutions by ensuring that the following considerations are adopted:

Coding Practices:

- An inventory of all locally developed applications should be maintained. This inventory should include at minimum the following information:
    - Application name
    - Primary business area and stakeholder
    - Application maintainer(s)
    - Infrastructure utilized, e.g. server(s), storage
    - Software dependencies, e.g. additional application, libraries, tools, etc.
- Applications should validate input properly and restrictively, allowing only those types of input that are known to be correct. Vulnerabilities to avoid include cross-site scripting, buffer overflow errors, and injection flaws.
- Applications should execute proper error handling so that errors will not provide detailed system information, deny service, impair security controls or create infrastructure instability

- Documentation should be included describing the security architecture of the application, including how data is classified and protected
- Applications should ensure that College data is categorized in accordance with the *Data Classification Policy*
- Applications processing Confidential or sensitive data shall ensure that all protection and strong encryption requirements set forth in the College's *Data Protection Policy* are met for storage, transmission, and retention
- Applications should make use of secure storage for College data (also see *Cloud Storage Policy*)
- Applications deployed on local servers should ensure setup and configuration in accordance with the provisions of the *Computer & Server Security Standards*
- Application logs should be implemented to the extent practical and ensure that sufficient error and security monitoring details are included to aid in follow-up analysis
- All applications shall incorporate the essential stages of analysis, design, planning, and quality assurance
- Security risk assessment should be performed by the Information Security Office as a component of the software design process
- Code-level security reviews must be conducted and documented (especially those which involve the collection, use or display of Confidential or sensitive data). These reviews should ensure that steps are taken to prevent fraud, including separation of duties, and any application dealing with financial or personally identifiable information should include review involving entities external of the development team.
- Security scans of new or modified applications shall be performed by the Information Security Office as part of quality assurance testing
- Applications which are obsolete or dependent on insecure supportive operating systems or application software should be removed from service or possible execution
- Change management processes shall be adopted and maintained for changes to existing software applications (see *Change Management Policy*)

- Third party involvement in application development or maintenance should be in accordance with the College's *Third Party Management Policy*

Application, Authentication and Authorization:

- Application development, production and administrative environments should ensure appropriate controls and practices are in place and observed to ensure secure operation and access. Any remote access requirements should be in accordance with the College's *Remote Access Policy*.
- Application authentication and authorization rules and processes, including access granting and revocation, shall be clearly documented
- Applications performing authenticating for access control should leverage the College's central authentication system
- Applications should leverage, where applicable and to the extent possible, role-based access authorized by affiliation, membership, and role, as opposed to access authorized by individual
- Periodical reviews of application authorizations should be performed on at least a semi-annual basis. This review should ensure removal or appropriate modification of authorizations for individuals who have left the College, transferred to other departments, or assumed new job duties within departments.
- Application authorization reviews should be automated to the extent possible

COMPLIANCE

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

EXCEPTIONS

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

Application Software: Computer software designed to perform a set of designed functions, tasks or activities to fulfill a business or operational requirement.

Confidential Data: Specifically restricted data from open disclosure to the public by law is classified as Confidential Data. Confidential Data requires a high level of protection against unauthorized disclosure, modification, transmission, destruction, and use.

Strong Encryption: Strong encryption is provided by well-established encryption algorithms, e.g. AES, SSL, which utilize long cryptographic keys, typically 256 bits or longer.

User: Any Washtenaw Community College faculty, staff, students or partner who has been authorized to access any College electronic information resource.

REFERENCES

Change Management Policy

Cloud Storage Policy

Data Classification Policy

Data Protection Policy

Remote Access Policy

Server and Computer Configuration Standards

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