**Deschutes County Information Technology Policy No. IT-3**

**Effective Date: May 1, 2025**

# Custom Software Development Standards

## STATEMENT OF POLICY

This policy provides a unified set of guidelines for coding, security, and privacy standards for custom software at Deschutes County. It aims to establish code quality and maintainability, protect sensitive data, prevent unauthorized access, and ensure compliance with relevant regulations and industry best practices.

## DEFINITIONS

*Changes in code development* - Changes in code development refer to modifications made to existing code, that can include enhancements, bug fixes, or refactoring efforts to improve the codebase.

*Change Release Advisory Board (CRAB)* – A group comprising IT managers responsible for approving and scheduling changes identified as medium or major risk.

*Custom Software* - Custom software development refers to the process of designing and creating software for a specific user, department, office, customer(s), or organization. It's different from off-the-shelf software, which is designed for the mass market.

*Data Classification* –Deschutes County data is classified into categories which are identified and described on the IT SharePoint intranet website.

*Developers* – Deschutes County employees, volunteers, contractors, third-party vendors, and others acting on behalf of the County who design, develop, maintain, and review custom-developed software code within the organization.

*Deschutes County IT* – The central IT Department for the County.

*New code development* - refers to the creation of software from scratch or the implementation of entirely new features or modules within an existing application.

*Peer code review* – The process by which a member of the Deschutes County IT Team reviews code to identify and address security vulnerabilities and ensure the code complies with the unified Development Standards prior to deployment. To request a peer review, please email helpdesk@deschutes.org.

*Risk Assessment Form* – This form can be found on the Information Technology SharePoint intranet website. It is created, maintained, and managed by the Deschutes County IT Team and used to assess and document the risks of proposed changes to new or existing code.

*Software code* – For the purposes of this policy, Deschutes County IT defines software code as a collection of instructions written in a programming language, which has been converted from human-readable source code into machine-readable instructions by a compiler. These instructions guide a computer or device in executing specific tasks.

*Software decommissioning* – Software decommissioning refers to the process of retiring a software application or system that is no longer needed or is being replaced by a new solution. This involves a series of planned steps to ensure that the software is safely and effectively removed from operation while preserving any necessary data and minimizing disruption to users.

*Software inventory* – A list of software applications and information can be found on the Information Technology SharePoint intranet website accessible to all IT employees. This inventory list is administered by the Deschutes County IT Team and maintained by Developers.

## APPLICABILITY

This policy applies to all officials, employees, volunteers, contractors, third-party vendors, and others acting on behalf of the County who are involved in the development, maintenance, and review of software code utilized within the organization.

## POLICY

These practices ensure consistency and quality in software, which streamline collaboration and reduce errors. They enhance security by minimizing vulnerabilities and requiring proper data classification and risk assessments for all changes.

### Development Standards

To follow established guidelines and best practices, developers must adhere to unified development standards established by the Deschutes County IT Team, which are accessible on the Information Technology SharePoint intranet website.

These documents, maintained and regularly updated by the Deschutes County IT Team, include language-specific coding standards, naming conventions, code structure, commenting, and best practices for supported coding languages.

### Supported Languages, Frameworks, And Development Tools

Developers must work with compatible and approved technologies. The list of supported items can be found on the Information Technology SharePoint intranet website. These standardized coding languages, frameworks, and development tools help streamline the development processes, improve code quality and security, and facilitate collaboration, leading to a more efficient, safer and effective software development processes. Using these standardized

resources will greatly reduce common vulnerabilities such as SQL injection, cross-site scripting (XSS), and buffer overflows.

**Identification of Stored Data**
All data handled by custom software must be classified according to its sensitivity (e.g., public, confidential, restricted) and documented on the Software inventory list. Appropriate security measures outlined in the Development Standards must be taken to protect data according to its classification level.

**Assessment of Risk**
All developers planning to create new code or modify existing code must complete a Risk Assessment Form. This form data will be evaluated using a model that categorizes business risk as minor, medium, or major. If the risk is classified as medium or major, developers must complete an additional form providing more detailed information, which will then be reviewed by the CRAB. Additionally, for medium and major changes, the CRAB will assign Deschutes County IT staff to conduct a peer review.

## PROCEDURE

To ensure that all software development aligns with established standards and practices—promoting quality, security, and compliance—specific steps must be followed. New code development, changes in code development, and software decommissioning steps are required to be followed and are detailed on the Information Technology SharePoint intranet website.

## TEMPORARY DEVELOPER SUPPORT

If a department or office experiences the absence of a developer, whether due to a vacancy or vacation, the Deschutes County IT Team may provide temporary support for the application, contingent upon the application's compliance with our processes, procedures, development standards, and the availability of IT resources. This assistance may continue, if resources allow, until a new developer is hired or the current one returns.

## COMPLIANCE AND ENFORCEMENT

**Legacy Code**
Any existing code prior to the effective date of this policy will be grandfathered for a period of three years. During this time, it will be exempt from immediate compliance with these policy requirements, unless security concerns arise or there is an identified business need. However, all medium or major updates or changes, modifications, or new deployments made after the policy's effective date must adhere to this policy.

**Oversight**
Ad-hoc peer code reviews may be conducted at the discretion of the Deschutes County IT Department to ensure compliance with this policy. Any violations identified will be reported to the Developer. The Deschutes County IT Team will work with the developer to provide

suggestions for corrections and establish a timeline for implementing the necessary adjustments. If the violations are not resolved within the specified timeframe, the Deschutes County IT Director and Department/Office Head will be notified.

Department/Office Heads are responsible for assessing business needs within their units to make informed decisions regarding software code development. This responsibility includes understanding and assuming the associated risks and liabilities, such as resource allocation, code issues that impact business, compliance considerations, and long-term support. They must also ensure that all development staff are aware of and adhere to the organization's development standards. Department/Office Heads are accountable for enforcing this policy and ensuring that any violations are promptly addressed and corrected.

Non-compliance with this policy may result in removal of the application, disciplinary action, up to and including termination of employment, and legal consequences, if laws are violated.

**Third Party Vendors or Contractors**
Contracts with third-party vendors or contractors for custom developed software as defined in this policy must include all specific security, procedures, and privacy requirements in this policy, including the right to audit and meet security incident reporting obligations.

**Exceptions or Deviations**
Any exceptions or deviations from this policy must be approved by the Department Head of the requestor and the Information Technology Director. Requests for exceptions can be sent via email to helpdesk@deschutes.org.

Approved by the Deschutes County Board of Commissioners on April 9, 2025.

_____
Nick Lelack, County Administrator