UNIVERSITY OF SOUTH DAKOTA

Policy Number: 5.015
Originating Office: Information Technology Services
Responsible Executive: Chief Information Officer
Date Issued: 2/10/2025
Date Last Revised: 2/10/2025

Secure Software Development

Policy Contents

I. REASON FOR THIS POLICY

The purpose of the Secure Software Development Policy is to ensure that software development, implementation, and maintenance adhere to industry best practices, meet University regulatory requirements, and incorporate information security through the software life cycle.

II. STATEMENT OF POLICY

The University of South Dakota (USD) Information Technology Services (ITS) is responsible for developing, maintaining and participating in Systems Development Life Cycle (SDLC) Standards for all USD systems development and implementation projects. All USD entities engaged in systems development or implementation activities must follow USD's Application Software Security Policy.

A. All application development must comply with the ITS Application Software Security Policy and the University Systems Development Lifecycle (SDLC) Policy.

B. This policy does not apply to student coursework or research-based software which is not public facing.

C. All in-house development that creates, manages, uses or transmits Restricted Data, as outlined in USD's Data Classification Categories, must be developed and maintained by USD Information Technology Services or Institutional Research. Exceptions must be approved by the Chief Information Officer or Chief Information Security Officer.

D. Non-ITS in-house developers must have projects reviewed and approved by ITS.

E. Student employee developers must be supervised by ITS and comply with ITS Policies and Procedures.

F. All third-party software development must be reviewed and approved by ITS and must comply with ITS Policies and Procedures.

III. DEFINITIONS

Development Workstation: Computer or computing environment specifically configured for use by developers to write, test, and debug software.

Systems Development Life Cycle (SDLC): A documented process for developing, implementing, and retiring information systems, ensuring security is integrated at every stage.

In-House Development: Software creation, modification, or maintenance by a USD employee.

Third-Party Development: Software creation, modification, or maintenance by an external vendor.

Risk Analysis: The process of identifying, assessing, and prioritizing potential risks which could affect the security, functionality, and success of a software project.

IV. PROCEDURES

Before development by a non-ITS entity begins, a software development plan must receive ITS approval. This plan should encompass:

- A comprehensive list of requirements
- A detailed design with milestones
- A complete list of relevant data elements
- Development, quality, and acceptance testing plans
- Risk analysis
- Implementation strategy
- Post-implementation maintenance, replacement, and retirement plans and review procedures

All in-house development work must be done on USD-owned equipment which meets USD's security requirements for development workstations.

V. RELATED DOCUMENTS, FORMS AND TOOLS

USD Policy 5.003 Information Security and Data Responsibilities

USD Application Software Security Policy

USD ITS Software Development Life Cycle (SDLC) Policy

USD Network Access Policy 5.011

SDBOR Policy 7.4 Security of Information Technology Systems