



## **Secure Software Development Lifecycle (Standard)**

Version 0.1

## Table of Contents

### Document Classification: University Confidential

Physical and Administrative Controls	Reproduction	Distribution	Destruction/Disposal
Each employee is responsible for controlling usage and access on a need-to-know basis. This policy also applies to contractors.	Limited copies may be made only to employees or contractors who have signed a non-disclosure agreement.	Internal: Use University envelope whenever possible. External: Use sealed envelope.	Use document destruction bins. Shred or erase magnetically recorded documents if unable to recycle.

### Document Revision

Date	Revision	Revised By	Basis for Revision & Description

### Document Change/Correction Request

Your feedback is valuable. Anyone who uses this document is invited to use this form to submit requests for changes or corrections to this document. Please complete all of the sections and mail to:

### Document Identification

**Document title**  
**Date of Document**  
**Master File Location**

### Requester Identification

Name	
Department	
Phone Number	( ) -
Email Address	

### Request

The following Change is requested:

Please describe the change and reason(s) why the change is requested.

Correction:

Section \_\_, page \_\_ contains the following erroneous information:

This information should be changed to:

Attach additional sheets if necessary to fully describe the change or correction.

## **1.1 Overview**

Information security must be integrated into new application and systems development from their inception and throughout the development lifecycle. The development lifecycle is defined as a period that begins with conception of a new development project and ends with retirement or removal of the developed software from all active use.

A development lifecycle typically includes five phases, irrespective of development methodology:

- Initiation
- Development/acquisition
- Implementation
- Operation/maintenance
- Disposal

## **1.2 Roles and Responsibilities**

### **Information Systems Director**

- Publishes and maintains policy guidelines for security in the applications life cycle.

### **Information Security Officer (ISO)**

- Prepares policy guidelines for building security into development lifecycles
- Ensures the plan for any particular development project includes security in all lifecycle phases
- Assists application developers/owners in addressing security requirement for each development lifecycle phase

### **Application Developers/Owners**

- Understands and defines the security requirements for each development lifecycle phase
- Implements security requirements when developing or modifying any software
- Documents security controls required by security plan

## **1.3 Development Lifecycle Security Procedures**

There are specific security requirements for each phase of the software development lifecycle:

### 1.3.1 Initiation

- The ISO and development manager conduct a sensitivity assessment that evaluates the sensitivity and criticality of the information to be processed by the planned software, as well as the system itself
- The assessment shall consider the following information and system needs, as prescribed by laws, regulations, and internal policies:
  - Information security
  - Information privacy
  - Information availability
  - Information integrity
  - Information confidentiality
  - System continuity, based on environment and public threats to the system or information should also be considered

### 1.3.2 Development/Acquisition

- The development team should work with the ISO to develop software security requirements at the same time they are defining the software requirements
- The development director/manager and ISO must ensure security requirements are incorporated into software design specifications
- If the software under development has been acquired in whole or part from another source—whether a vendor, other third party, or previous internal development effort—the development manager and ISO should include procedures that ensure security features in the acquired software meet security requirements and, as much as possible, adhere to internal security development standards.

### 1.3.3 Implementation Phase

- The development team must ensure that software security features are properly configured and enabled
- The development team must test security functionality prior to software release
  - Security testing should be performed under conditions as close to production conditions as possible

### 1.3.4 Operation/Maintenance Phase

- The development team must complete all security activities required by UTO, the software development plan, and the universities Information Security program. These activities might include software and data backups, user training, access management workflows, and system reviews.

### **1.3.5 Disposal Phase**

- The development or IT team moves to another system, archives, discards, or destroys application code
- Hardware and software can be sold, given away, or discarded. It staff should ensure that all media has been sanitized to prevent the unintended leakage of confidential information, prior to transferring or discarding
- Disposition of licensed software must meet requirements of the software license or other relevant agreements.

### **1.4 Enforcement**

Violation of this policy can result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Arizona State University ACD 125 access privileges, civil, and criminal prosecution.

### **1.5 Supporting Documentation**

This Standard is supported by the following rules, standards, and procedures:

- [Link to ACD 125](#)
- [Link to Data Classification](#)
- [Link to University Information Security Policy](#)
- [Link to ASU Privacy Policy](#)
- [Link to Encryption Standard](#)
- [Link to Information Security Standard and Measures](#)

### **1.6 Policy Support Contact**

- Information Security Officer

### **1.7 Resources**

- [Federal Agency Security Practices](#), US Government, National Institute of Standards and Technology (NIST)
- ASU [Information Security Awareness Site](#)