# Secure Coding Guidelines and Training Policy

## Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, the Office of Information Security has established a formal policy and supporting procedures concerning software development and secure coding guidelines and training. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

## Policy

The Office of Information Security will ensure that the software development and secure coding guidelines and training policy and procedures adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Software developers and all other relevant personnel involved in the development of software for the University of South Alabama are required to undergo annual training in secure coding techniques for the software platforms(s) with which they work.
- Software developers and all other relevant personnel involved in the development of software for the University of South Alabama are required to submit their Secure Coding Training checklist on an annual basis as evidence that they are knowledgeable in secure coding techniques.
- Software developers involved in the software development process will adhere to professional guidelines, such as the Open Web Application Security Project (OWASP) Code of Ethics and CWE/SANS.
- The Office of Information Security's software development lifecycle includes policies, processes and procedures to ensure that internally-developed applications are not vulnerable to the following threats:
    - Injection Flaws (SQL, OS and LDAP Injection)

- Buffer Overflows
- Insecure Cryptographic Storage
- Insecure Communications
- Improper Error Handling
- All high risk vulnerabilities identified in the vulnerability identification process as found in the Risk Ranking Table within the Security Patch Management Installation Policy and Procedures document.
- Cross-Site Scripting
- Improper Access Control
- Cross Site Request Forgery
- Broken Authentication and Session Management
- All "High" vulnerabilities and threats as identified in the Risk Ranking Table found in the Security Patch Management Installation Policy and Procedures.

## Responsibility for Policy Maintenance

The Office of Information Security is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

## Revision History

February 8, 2019 (Policy Created)

July 15, 2019 (Policy Modified)

Adapted from Stanford University's PCI DSS Policies 1-2019