MedTech Industries

Software Development Lifecycle Standard Operating Procedure

Purpose: This document aims to provide a detailed overview of the company's System Development Lifecycle (SDLC) program, including sub-processes to explain how software is conceptualized, developed, and maintained.

The SDLC works to ensure that computerized systems are fit for intended use, meet business requirements, and are compliant with applicable regulations. The SDLC is a framework for initiating, developing, implementing, and operating information systems and applications. MedTech industries has adopted and modified the SDLC framework from NIST.

Initiation

This phase seeks to obtain and analyze requirements, assess compliance requirements, and assess risks of the business requirements. The key activity in this phase is preparing the requirements specification in consultation with the Payroll System Owner.

During the initiation phase, the organization confirms the need for a system and notes its purpose. Security planning should begin in the initiation phase by identifying critical security roles to be carried out in the system's development. Then, for security reasons and requirements, the information to be processed, transmitted, or stored receives an evaluation, and all stakeholders should have a shared understanding of the security details.

Development

The system is planned, purchased, programmed, developed, or otherwise built during this phase. A critical security activity in this phase is performing a risk assessment and using the results to augment the baseline security controls. In addition, the organization should examine security requirements, conduct testing, ready the initial documents for system certification and accreditation, and create the security architecture.

Implementation

In the implementation phase, the organization customizes and enables system security features, tests the functionality of these features, installs or executes the system, and receives formal authorization to use the system. In addition, if the application or the support system receives new controls, it will be necessary to perform additional acceptance tests of those new controls. This process guarantees that new controls meet security specifications and do not clash with or invalidate existing controls. Fully

document the results of the design reviews and system tests, revise these findings as new reviews or tests are performed, and maintain the details in the organization's official records.

Operations and Maintenance

In this phase, systems and products are established and running, enhancements or changes to the system are created and tested, and hardware and software components are added or substituted. The organization should continuously monitor the system's performance to ensure that it is consistent with pre-established user and security requirements and that necessary system modifications are incorporated.