Software Development Life Cycle Policy and Procedures

Overview

This document is for exclusive use by MSLA.

Version	Description [or description of changes]	Author	Creation date	Approved by	Date approval
1.2	Updated version	MSLA IT Department	06/22/2021	Luis Rios	06/12/2021

TABLE OF CONTENTS

Purpose

This policy defines the overall conceptual development and implementation requirements for MSLA International products. The policy applies to all MSLA International employees and other individuals and organizations who perform any software or systems development work under MSLA International´s supervision.

The purpose of this policy is to provide a clear methodology to help ensure the successful implementation of software projects advancing MSLA International's business objectives. The procedures below provide a structure to allow executive leadership, other management, and other contributors to sign off on software/systems requirements and implementation.

The software development life cycle phases described in greater detail below are:

- Requirements analysis
- Architecture and design
- Testing
- Deployment and implementation
- Operations and maintenance
- Decommissioning

The descriptions of the steps in each phase are not intended to be rigid and inflexible or to be followed in a particular order in every case. Rather, these are guidelines for consideration and action.

Procedures and phases

1. **Requirements analysis**

   The following activities make up the requirements analysis phase:

   - Analyze business requirements
   - Perform a risk assessment
   - Discuss security-related aspects of project and determine security solution requirements
   - Review applicable legal/regulatory and MSLA International policy requirements
   - Analyze and incorporate program management items, such as timeframes

- Consider “buy v. build” aspects of requirements
- Assess cost and budget constraints, and approve budget

2. **Architecture and design**

The following activities make up the architecture and design phase:

- Ensure development teams are aware of requirements, including security requirements
- Develop and/or refine overall architecture
- List technical controls applicable to project
- Perform architecture walk-through
- Create system-level design
- Perform cost-benefit analyses based on approved requirements
- Perform full design review, including technical reviews of application, infrastructure, and processes
- Design initial end-user training and awareness programs
- Update MSLA International policies, standards, and procedures if necessary
- Assess and document how to mitigate residual vulnerabilities, if any

3. **Development**

The following activities make up the development phase.

- Set up a secure development environment
- Train infrastructure teams on installation and configuration of applicable software
- Develop code for application-level components
- Set up vulnerability-tracking processes, including a security test plan as needed
- Conduct unit testing and integration testing

4. **Testing**

   The following activities make up the testing phase.

   - Perform a code and configuration review, through both static and dynamic analysis of code to identify problems
   - Test configuration procedures
   - Perform system tests, including performance and load tests with security controls enabled
   - Perform usability testing
   - Conduct overall security vulnerability assessment based on work to date

5. **Deployment and implementation**

   The following activities make up the deployment and implementation phase.

   - Conduct pilot deployment, including all relevant components
   - Conduct transition between pilot and full scale deployment
   - Perform integrity testing on system files to ensure authenticity
   - Deploy training and awareness programs
   - Require participation of at least two developers to conduct full scale deployment to production environment

6. **Operations and maintenance**

   The following activities make up the operations and maintenance phase.

   - Administer users and access
   - Tune performance as needed
   - Perform regular backups and other system maintenance
   - Conduct ongoing training and awareness
   - Conduct vulnerability and risk assessments in accordance with applicable MSLA International policies

- Review operational systems on an ongoing basis for performance purposes, with documentation and resolution of problems as needed
- Develop regular patching process

7. **Decommissioning**

   The following activities make up the decommissioning phase.

   - Conduct necessary testing of remaining system components after component/software removal
   - Determine data retention requirements in accordance with applicable MSLA International policies
   - Document the technical security design
   - Update MSLA International policies, standards, and procedures if necessary
   - Assess and document how to mitigate residual vulnerabilities, if any

Waivers

Waivers from certain policy provisions may be sought following the MSLA International Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.