**Secure Development Lifecycle Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_mj0nqc27m79) **4**

[**Scope**](#_q5cb4feagdxg) **4**

[**Policy**](#_purs9pvjc6g3) **4**

[**SDLC Standards**](#_8fc3sfesqhda) **4**

[**System Initiation Phase**](#_xeyvjxm75ox0) **4**

[**System Requirements Analysis Phase**](#_qjprv61mzhyu) **4**

[**System Design Phase**](#_jojfw79tv3cv) **5**

[**System Construction (Procurement) Phase**](#_yn18sulac5sd) **5**

[**System Testing and Acceptance Phase**](#_x1vbavhtbq4q) **5**

[**System Implementation Phase**](#_z9yjyzqobwp3) **6**

[**System Maintenance Phase**](#_8fsk94cg323) **6**

[**System Archival Phase**](#_axnw7uw8lk82) **6**

[**Correct processing in applications**](#_3dkam4tvr0jp) **6**

[**Security of system files**](#_ofn1a51emw63) **7**

[**Change, Review, and Update**](#_w1o88vxspwq8) **7**

[**Disciplinary Action**](#_mm5ewidk84i8) **7**

[**Responsibility**](#_4b3sf8bveob9) **7**

[**Related Documents**](#_tmup0okkxrpf) **8**

# 

# **Purpose**

The purpose of the SDLC Policy is to describe the requirements for developing and implementing new *[Company]’s* software and systems. In addition, the process provides visibility of the design, development, and implementation status needed to ensure delivery on time and within budget.

# **Scope**

The scope of this policy includes all employees, contractors, and temporary workers involved in the development of software or systems.

# **Policy**

* All development work must have a separation between production, development, and test environments.
* Development and QA staff must not be permitted access to production systems unless required by their respective job duties/descriptions.
* The vulnerability management and penetration tests should be conducted.

## **SDLC Standards**

### **System Initiation Phase**

* The Initiation phase is when proposals should be identified and the decision made to commit the necessary efforts and resources to resolve needs and proposals.
* The initial steps in information gathering should be performed defining the project objectives, stakeholders, milestones, deliverables, roles and responsibilities, resources, risks, assumptions and constraints, high-level scope, and requirements.

### **System Requirements Analysis Phase**

* The System Requirements Analysis is the phase where product and project information should be gathered and investigated.
* The requirements should be clearly defined in this phase and the project planning is performed.
* The documentation regarding this phase should be reviewed and all the necessary clarifications, corrections, and issues should be processed properly.
* The project and test planning activities may be started in this phase with the preparation of the scope, requirements, communication, and change management plans.

### **System Design Phase**

* During the Design phase, the product system architecture should be elaborated.
* In this phase, the architecture should define the components, their interfaces, and behaviors.
* The decisions on the programming technologies, environments, software and hardware, packages, applications, memory size, platform, algorithms, data structures, global type definitions, interfaces, and many other engineering details should be also taken.
* The configuration aspects should be documented and the build delivery processes should be established here as well.
* Security Requirements should be included in the System Design Phase based on the best security practices or standard-based required security recommendations (e.g. OWASP, NIST, etc.)

### **System Construction (Procurement) Phase**

* This phase validates the transformation of the detailed design documents into a finished product or solution.
* Manual and automated testing at a unit or module level is done throughout this phase by the system or software developers. Security considerations are taken into account during testing.
* A third-party product may be utilized as a system or software solution to best fit the user requirements and is more practical from a budgetary and resource perspective.

### **System Testing and Acceptance Phase**

* This phase should validate or confirm that the developed system or software meets all functional requirements as captured during the System Requirements Analysis Phase.
* Representatives separate from the development group should conduct internal Quality Assurance (QA) testing.
* The responsible person should conduct user acceptance testing.
* Documentation during testing should be detailed and contain descriptions and results of all testing processes at each stage.
* Final security assessment testing is now conducted.
* Any problems identified during the previous phases must be resolved or remediated before implementation.

### **System Implementation Phase**

* The final stage of initial development, where the software is put into production and runs actual business.
* The finished, tested, and user-accepted system or software is moved from the testing environment to production.
* All tools, code, or access mechanisms used for the development or testing of the system or software must be removed from the software that is being moved into a production environment.

### **System Maintenance Phase**

* This phase is the ongoing life of the system or software. Unlike the other phases, this phase only ends when the system or software is decommissioned.
* A customer/user support structure and any other necessary operational support processes should be in place.
* Any planned changes to the system or software should be scheduled, communicated, and documented.
* Continuous security penetration testing is conducted on the system or software throughout its life cycle at regularly scheduled intervals (at a minimum annually).
* Mandatory security testing is conducted when any major configuration or architecture change is made.

### **System Archival Phase**

* All the project-related data and/or project software artifacts should be archived or deleted according to the predefined procedures.
* The objects prepared for archiving should be saved with the proper access control in a secure storage place.

## **Correct processing in applications**

* The company’s system acquisition/development methodology should ensure that appropriate input data validation controls are existing/built-in in the systems before their deployment in the production environment.
* Data integrity protection requirements in the applications and information systems should be identified and controls for data integrity should be implemented.
* Data output from an application system should be validated to ensure that the processing of stored information is correctly processed and appropriate to the business logic.

## **Security of system files**

* Appropriate applications should be implemented to deploy the software on operational/production systems to minimize the risk of corruption of these systems.
* Access to installed software on operational/production systems should be restricted to authorized personnel only.
* Modifications to the operational environment should be logged and previous versions are maintained for contingency/rollback purposes.
* The production system should hold only the production version of the code.
* Production versions of code should be implemented in the operational/production environment only after successful completion of testing and user acceptance of the system in a staging environment.
* Access to program source code and associated items should be strictly controlled.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. IT Manager shall exclusively perform changes to this policy.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. *[Company]’s* management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Change Management and Control Policy
* Vulnerability Management Policy