Software Development Life Cycle (SDLC) Policy

July 2021

Contents

Review History

Date of this Review: 07/07/2021	Date of next review: 07/07/2022

Document Location

Website – Resources > Policies & Guidelines

Review Result

Reviewed By:	Debasish Dutta
Issued Date:	07/07/2021
Approved By:	Rajesh Bhuyan
Revision No.:	0

This Policy was approved by Director, trustea Sustainable Tea Foundation. It shall be reviewed and, as necessary, amended by the Institute annually. All amendments shall be recorded on the revision history section above.

1. SCOPE AND PURPOSE

This policy defines the development and implementation requirements for Trustea Sustainable Tea Foundations' (tSTF) custom software applications. This policy applies to all employees at (tSTF) and other individuals and organizations who work with any form of software or system development under the supervision of tSTF.

The purpose of this policy is to provide a methodology to help ensure the successful implementation of systems that satisfy tSTF strategic and business objectives. This documentation provides a mechanism to ensure that executive leadership, functional mangers, and users (where appropriate) sign-off on the requirements and implementation of systems. The process provides visibility of the design, development, and implementation status needed to ensure delivery on time and within budget.

2. POLICY STATEMENT

Policy Goals:

- Deliver quality systems which meet or exceed stakeholders' expectations when promised and within cost estimates
- Provide a framework for developing quality systems using an identifiable, measurable, and repeatable process
- Identify and assign the roles and responsibilities of all involved parties, including functional and technical managers, throughout the system development life cycle
- Ensure that system development requirements are well defined and subsequently satisfied.

Policy Objectives:

- Establish appropriate levels of management authority to provide timely direction, coordination, control, review and approval of the system development project
- Document requirements and maintain traceability of those requirements throughout the development and implementation process
- Ensure that projects are developed within the current and planned information technology infrastructure.

3. SEGREGATION OF ENVIRONMENT

- Development will be performed in a dedicated network zone, separate from quality assurance and production.
- Quality Assurance will be performed in a dedicated network zone separate from production and development.

4. SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) PHASES

Initial Phase

The purposes of the Initiation Phase are to:

- Identify and validate an opportunity to improve business accomplishments or a deficiency related to a business need
- Identify significant assumptions and constraints on solutions

- Recommend the exploration of alternative concepts and methods to satisfy the need

Feasibility Phase

The Feasibility Phase is the initial investigation or brief study of the problem to determine whether the systems project should be pursued. A feasibility study establishes the context through which the project addresses the requirements and investigates the practicality of a proposed solution. The feasibility study is used to determine if the project should get the go-ahead. If the project is to proceed, the feasibility study will produce a project plan and budget estimates for the future stages of development.

Requirements Analysis Phase

This phase formally defines the detailed functional user requirements, using high-level requirements identified in the Initiation and Feasibility Phases. In this phase, the requirements are defined to a sufficient level of detail for systems design to proceed. Requirements need to be measurable, testable, and relate to the business need or opportunity identified in the Initiation Phase.

Design and Development Phase

During this phase the system is designed to satisfy the functional requirements identified in the previous phase. Since problems in the design phase can be very expensive to solve in later stages of the software development, a variety of elements are considered in the design to mitigate risk. These include:

- Identifying potential risks and defining mitigating design features
- Performing a security risk assessment
- Developing a conversion plan to migrate current data to the new system
- Determining the operating environment

Implementation, Documentation and Testing Phase

For Trustea Sustainable Tea Foundation’s applications, as part of the implementation phase, updated detailed documentation will be developed and will include all operations information needed by the users, including detailed instructions for when systems fail. Trustea Sustainable Tea Foundation’s applications may not be moved into the production environment without this documented information.

Testing will be performed in its own environment and includes unit, integration, and system testing to ensure the proper implementation of the requirements.

The requirements will be documented and will then be tested. All components deployed for cloud architecture are based on a defined secure standard from the vendor and security best practices and goes through a change control process that includes configuration, testing, and QA, before it is deployed in Production.

Operations and Maintenance Phase

System operations and maintenance is ongoing. Trustea Sustainable Tea Foundation conducts an annual review with Stakeholders. The system is monitored for continued performance in accordance with user requirements and needed system modifications are incorporated when identified, approved, and tested. When modifications are identified, the system may re-enter the planning phase.

Security Vulnerabilities

Managing the security vulnerabilities will be handled by the IT Team, who will identify, manage, and minimize the security vulnerabilities by code fix or configuration change (for example, by a hotfix, patch, or other way of handling the security vulnerabilities). Trustea Sustainable Tea Foundation has a security patch policy including evaluation and definition of the severity. Critical patches are assessed and evaluated within 5 business days and implemented as soon as possible. Priority certification and full QA testing is employed to validate the full system functionality and availability of the systems post-patching. Refer to the ongoing security patches based on ***trustea Security Patches and Vulnerability Assessments Policy*** (Appendix - A).

5. POLICY REVIEW

This policy will be reviewed at least annually by Management for effectiveness and to ensure its continued use and relevance as part of the Trustea information security management system (TISMS).

6. POLICY ENFORCEMENT

Failure to comply with this policy will result in disciplinary action up to and including termination of engagement.

APPENDIX – A

Ex Libris Security Patches and Vulnerability Assessments Policy

Introduction

Trustea Sustainable Tea Foundation (tSTF), considers the security of its products a high priority. As such, tSTF continually seeks to ensure that its solutions do not contain vulnerabilities that may compromise the security of its products.

As part of ongoing efforts by Trustea Sustainable Tea Foundation to provide secured solutions that help stakeholders maintain the integrity of their environment, the company has implemented a security assessment process for software components used with Trustea Sustainable Tea Foundation's products and security patches and vulnerabilities.

This security assessment process comprises of four stages: Monitoring, Assessment, Remediation, and Communication. These stages are explained below.

Monitoring

Underlying the entire security assessment process, the security team—led by the trustea IT Manager (ITM)—continuously monitors and evaluates the security of Trustea Sustainable Tea Foundation's software applications, as well as third-party releases and patches. This ongoing monitoring ensures a fast response when security issues arise. The team proactively tracks new third-party releases and roadmap announcements together with security alerts and patches, ensuring a consistently rapid response and proactive approach to products' security.

Assessment

Each new software version is assessed by Trustea Sustainable Tea Foundation to determine its suitability to the functionality, stability, and security of the relevant Trustea Sustainable Tea Foundation's applications. Based on this software assessment, a decision is made with respect to the software version to be certified.

Remediation

For security patches and vulnerabilities, Trustea Sustainable Tea Foundation may recommend configuration changes rather than patch installation, as described in the table below.

Classification of Severity Level	Remediation Action
Critical Critical severity patches and reported vulnerabilities will be **assessed as soon as possible** (within five business days): • after the official release by the vendor Or	Announcement of the availability of Trustea Sustainable Tea Foundation provided Hot Fix or patch as soon as possible Or recommendation for configuration changes

Classification of Severity Level	Remediation Action
• from the moment they were reported to or discovered by trustea IT Manager	
High and Medium High and Medium severity security patches and reported vulnerabilities will be assessed **within two weeks:** • from their official release by the vendor Or • from the moment they were reported to or discovered by trustea IT Manager.	Incorporate the fix into next service pack Or recommendation for configuration changes
Low Low severity security patches and reported vulnerabilities will be assessed within **one month:** • from their official release by the vendor Or • from the moment they were reported to or discovered by trustea IT Manager.	Incorporate the fix into next minor or major release Or recommendation for configuration changes

Communication

Trustea Sustainable Tea Foundation will update stakeholders on any security issue. Security advisories will be published in the web portal > IT initiative section, in the Trustea Sustainable Tea Foundation's official portal. Trustea encourages all stakeholders to review the registered Security advisories to ensure that the right person receives the security information.

trustea Sustainable Tea Foundation

6, Southern Avenue,

5th Floor,

Kolkata – 700026, WB,
India

Telephone + 91 9830563511
E-mail dutta@trustea.org, admin@trustea.org