This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Secure Systems Development Life Cycle Policy Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This policy aims to define cybersecurity requirements related to <organization name>'s Secure Systems Development Life Cycle (SSDLC) process. The policy intends to set the appropriate requirements to govern <organization name>'s systems and software development process in order to reduce the likelihood of cybersecurity attacks though poorly implemented designs and functionality. Integrating SSDLC good practices with <organization name>'s Information Technology (IT) project and change management processes will help reduce the number, to mitigate the impact and to address the root cause of vulnerabilities in system designs, configurations and software packages.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018 and CSCC-1:2019, in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy applies to all <organization name> systems, applications and software codes that are designed and developed in-house or using third parties, with a target audience of <organization name>'s personnel (employees and contractors).

Policy Statements

1. General Requirements

1-1 All SSDLC activities must be managed in compliance with <organization name>'s Information and Cybersecurity policies and related government regulations.

1-2 SSDLC policy and standards must be periodically reviewed and revised (as necessary) at least once a year.

1-3 SSDLC related training sessions and programs must be developed and delivered to relevant personnel.

1-4 An SSDLC project plan must be developed and tracked for progress against all <organization name>'s IT design, development and implementation activities.

1-5 A secure and automated process for checking, approving and promoting newly developed or updated functionality must be leveraged by <organization name> for any software development activities.

1-6 Solution architecture and security must be developed and reviewed as part of all IT projects.

1-7 Baseline system security configurations must be applied to all <organization name> systems and devices.

1-8 Component interfaces required for product/feature development must be evaluated prior to integration.

1-9 Secure coding practices must be adhered to on all development projects and will align with industry best practices.

1-10 Testing and quality assurance activities must be performed across development activities and must be iterative in approach.

1-11 Software developed must be tested prior to being moved into the production environment.

1-12 Security vulnerability tests must be conducted for all critical systems and software in the <organization name>'s IT environment.

1-13 <organization name> must prepare a proper plan to deal with all software related vulnerabilities and the mitigation actions required based on the criticality.

1-14 Any IT project plans must ensure that deployment strategies are authorized, traceable and secure.

1-15 Any IT projects must be subjected to ongoing monitoring activities to measure and monitor project performance.

1-16 All software and applications must be subject to ongoing monitoring when designing and implementing software solutions.

1-17 All systems and software which reach end of life span or are no longer required by <organization name> must be decommissioned according to <organization name> security and media disposal policies.

2. SSDLC Additional Requirements

2-1 Security risk assessments must be carried out for all <organization name> systems, software and applications in accord with IT project, change management and security processes, as per related laws and regulations.

2-2 Threats to <organization name> systems, applications and software development projects must be identified and appropriately mitigated, as per related laws and regulations.

2-3 Security-related requirements including data classification and access controls must be integrated into the system or application software designs.

2-4 Systems and applications must be deployed securely into the production environment.

2-5 Network segregation and zoning for <organization name> system and application environments must be adhered to.

2-6 Data and information protection controls must be used in all <organization name> systems and applications.

2-7 A configuration and change management protocol must be adhered to and followed.

2-8 A secure code scanning tool must be used on development code to identify security vulnerabilities for sensitive data sets and critical applications.

2-9 Emergency change procedures must be developed and implemented.

2-10 Third party involvement in development activities must be formally identified and managed.

2-11 Compliance with <organization name> policies and standards for all IT projects must be adhered to.

Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <information technology function> and <cybersecurity function>

4- **Policy Commitment Measure:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- <head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.

2- All personnel at <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.