System Development Lifecycle Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

Procedure Name DOCID: PR-IT-IS-16

Document Control

i. Document Identification

Document Title and Version:	**PR-IT-IS-16 System Development Lifecycle Procedure v1.0**
Effective Date:	5th October, 2019
Document Author:	Information Security Team
Owner:	CIO/Head of IT
Approved By:	

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor's (If Required)

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO	CIO/Head Of IT

v. Revision History

Rev	Date	Author	Description	Approved By	Initiated Date
0	05-10-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	13-12-2019
1	13-12-2019	Information Security Team	approval	Andy Chong	17-12-2019
2	22-10-2021	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	19-12-2021
3	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
4	27-09-2023	Information Security Team	Review and Updating – Period changed from annual to once every two years. Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
5	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
6	30-04-2024	Information Security Team	Re-branding	CIO/Head of IT	

Ncell	**Ncell**	Classification: Internal
	System Development Lifecycle Procedure	Owner: Information Security Team
		Effective Date: 5th May, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO: Andy Chong

Table of Contents

1. Purpose

The purpose of this procedure is to establish a risk management-based approach for systems and projects development and building means for integrating security early and throughout the established system.

2. Review and Updating

This procedure shall be reviewed annually or whenever significant changes occur in the organization.

3. Scope

This procedure shall be applicable to all employees of Ncell; as well as Third party vendors, contractors, partners, collaborators and any others doing business or research with Ncell will be subject to the provisions of this procedure. Any other parties, who use, work on, or provide services involving Ncell computers, technology systems, and/or data will also be subject to the provisions of this procedure.

4. System Development Lifecycle (SDLC)

4.1 Overview

A typical SDLC includes five phases: initiation, development/acquisition, implementation/assessment, operations/maintenance, and disposal. Each phase includes a minimum set of security tasks needed to effectively incorporate security in the system development process. Note that phases may continue to be repeated throughout a system’s life prior to disposal.

i. **Initiation**: During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

ii. **Development/Acquisition**: During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed.

iii. **Implementation/Assessment**: After system acceptance testing, the system is installed or fielded.

iv. **Operation/Maintenance**: During this phase, the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events.

v. **Disposal**: Activities conducted during this phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies.

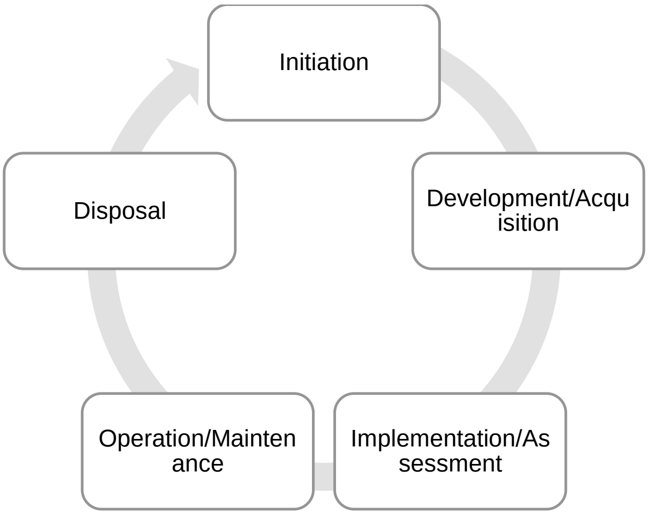

Figure 1: Secure Development Lifecycle

4.2 Key Roles and Responsibilities in SDLC

Axiata Role	Ncell Role	Responsibilities
Authorizing Official (AO)	Relevant CXO-1	An AO is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organization operations and assets, individuals, other organizations, and the Nation. To do this, the AO relies primarily on: (i) the completed security plan; (ii) the security assessment report; and (iii) the plan of action and milestones for reducing or eliminating information system vulnerabilities.
Head of IT	Head of IT	The Head of IT is responsible for the organization's information system planning, budgeting, investment, performance, and acquisition. As such, the Head of IT provides advice and assistance to senior organization personnel in acquiring the most efficient and effective information system to fit the organization's enterprise architecture.
Configuration Management (CM) Manager	Change Manager	The CM manager is responsible for managing the effects of changes or differences in configurations on an information system or network. Thus, the CM manager assists in streamlining change management processes and prevents changes that could detrimentally affect the security posture of a system before they happen.
Contracting Officer	Procurement Director	The Contracting Officer is the person who has the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.
Contracting Officer's Technical	Technical Lead	The COTR is a qualified employee appointed by the Contracting Officer to act as their technical representative in managing the technical aspects of a contract.
Information System Security Officer	Information Security and Privacy Officer	The Information System Security Officer is responsible for ensuring the security of an information system throughout its life cycle.
Legal Advisor/Contract	Legal Team	The legal advisor is responsible for advising the team on legal issues during the acquisition process.
Privacy Officer	Information Security and Privacy Officer	The privacy officer is responsible for ensuring that the services or system being procured meet existing privacy policies regarding protection, dissemination (information sharing and exchange), and information disclosure.
Program Manager/ Official	Project Manager	This person represents business and programmatic interests in the information system during the SDLC process. The program manager plays an essential role in security and is, ideally, intimately aware of functional system requirements.
QA/Test Director	Project Manager	The QA/Test Director is responsible for system test and evaluation, and functions as a resource across a variety of programs by assisting in the development and execution of test plans in conjunction with Program Managers and customers. This person reviews system specifications and determines test needs, and works with Program Managers to plan activities leading up to field test activities.
Chief Information Security Officer (CISO)	Information Security and Privacy Officer	The CISO, also known as Chief Information Security Officer, is responsible for promulgating policies on security integration in the SDLC and developing enterprise standards for information security. This individual plays a leading role in introducing an appropriate structured methodology to help identify, evaluate, and minimize information security risks to the organization.
Software Developer	Project Manager	The developer is responsible for programmatic coding regarding applications, software, and Internet/intranet sites, including "secure coding," as well as coordinating and working with the Configuration Management (CM) manager to identify, resolve, and implement controls and other CM issues.
System Architect	Technical Lead	As the overall designer and integrator of the application, the system architect is responsible for creating the overall design architecture and for maintaining the conceptual integrity of the architecture throughout the project life cycle. The System Architect is also responsible for ensuring

		the quality of technical work products delivered by the project team, including designs, specifications, procedures, and documentation.
System Owner	System Owner	The system owner is responsible for the procurement, development, integration, modification, operation, and maintenance of an information system.
Other Participants	Other Participants	The list of SDLC roles in an information system development can grow as the complexity increases. It is vital that all development team members work together to ensure that a successful development is achieved. Because information security officials must make critical decisions throughout the development process, they should be included as early as possible in the process. System users may assist in the development by helping the program manager to determine the need, refine the requirements, and inspect and accept the delivered system. Participants may also include personnel who represent IT, configuration management, design and engineering, and facilities groups.

4.3 Incorporating Security in SDLC

This section describes several security considerations that will help integrate information security into the SDLC. Security considerations are identified in each SDLC phase, thus advancing the business application and security requirements together to ensure a balanced approach during development.

4.3.1 SDLC Phase: Initiation

During this first phase of the development life cycle, security considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered.

Key security activities for this phase include:

- Initial delineation of business requirements in terms of confidentiality, integrity, and availability;
- Determination of information categorization and identification of known special handling requirements to transmit, store, or create information such as personally identifiable information; and
- Determination of any privacy requirements.

Security discussions should be performed as part of (not separately from) the development project to ensure solid understandings among project personnel of business decisions and their risk implications to the overall development project.

i. Initiate Security Planning

Security planning should begin in the initiation phase by:

a. Identifying key security roles for the system development;
b. Identifying sources of security requirements, such as relevant laws, regulations, and standards;
c. Ensuring all key stakeholders have a common understanding, including security implications, considerations, and requirements; and
d. Outlining initial thoughts on key security milestones including time frames or development triggers that signal a security step is approaching.
e. A series of milestones or security meetings should be planned to discuss each of the security considerations throughout the system development.

ii. Classification of Information Assets

a. The project manager in consultation with the concerned Section Manager should determine the Asset Owners and Asset Custodians.
b. The Asset Owner should then classify the information asset as per the organisation’s Information Classification Procedure.
c. Appropriate CIA rating should be determined for the information assets.

iii. Assess Business Impact

a. Identify lines of business supported by this system and how those lines of business will be impacted;
b. Identify core system components needed to maintain minimal functionality;
c. Identify the length of time the system can be down before the business is impacted (initial idea of the needed Recovery Time Objective); and
d. Identify the business tolerance for loss of data (initial idea of the needed Recovery Point Objective).
e. The BCP team should conduct a business impact analysis comprising for the new information systems in consultation with the concerned stakeholders.

iv. Ensure Use of Secure Information System Development Processes

a. The Project Manager shall ensure that Ncell's Secure Coding Guidelines are communicated to the development team.
b. A concept of operations document for secure development should be established.
c. System development should occur with standard processes that consider secure practices and are documented and repeatable.

4.3.2 SDLC Phase: Development/Acquisition

This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:

- Conduct the risk assessment and use the results to supplement the baseline security controls;
- Analyse security requirements;
- Perform functional and security testing;
- Prepare initial documents for system certification and accreditation; and
- Design security architecture.

i. Conduct Risk Assessment

a. The system owner shall conduct a risk assessment of the new information systems as per Ncell's Risk Management Procedure.
b. Results should show that specified security controls provide appropriate protections or highlight areas where further planning is needed.
c. Since this risk assessment is completed at a more mature stage of system development, there may be a need to revisit previously completed security steps, such as BIA or Security Classification.

ii. Comply with Ncell's Information Security policy, procedures and guidelines

a. Identify applicable security controls from the information security documentation.
b. Determine method and timelines for applying the information security controls.
c. Formulate a system security plan comprising of the above mentioned information.
d. The Project Manager and Technical Lead shall be responsible for designing and implementing the information security controls in consultation with the Information Security Officer.
e. The Information Security Officer shall be responsible for reviewing the implementation plan.

iii. Design Security Architecture

a. At the system level, security should be architected and then engineered into the design of the system by the Technical Lead.
b. This may be accomplished by zoning or clustering services either together or distributed for either redundancy or additional layers of protection.
c. Security designing at the system level should take into consideration services obtained externally, planned system interconnections, and the different orientations of system users (e.g., customer service versus system administrators).

iv. Engineer in Security and Develop Controls

a. During this stage, security controls are implemented and become part of the system rather than applied at completion.
b. Applying security controls in development should be considered carefully and planned logically. The intent is to integrate the controls so that challenges with system performance are known early.
c. Additionally, some security controls may limit or hinder normal development activities.
d. For new information systems, the security requirements identified and described in the respective system security plans are now designed, developed, and implemented.
e. The system security plans for operational information systems may require the development of additional security controls to supplement in-place controls or the modification of controls that are deemed to be less than effective.
f. During this task, decisions are made based on integration challenges and trade-offs. It is important to document the major decisions and their business/technology drivers.
g. In cases where the application of a planned control is not possible or advisable, compensating controls should be considered and documented.

v. Develop Security Documentation

a. While the most prominent document is the System Security Plan, documentation supporting it may include:
   I. Configuration management plan
   II. Contingency plan (including a Business Impact Assessment)
   III. Continuous monitoring plan
   IV. Security awareness, training and education (SATE) plan
   V. Incident response plan
b. Development of these documents should consider the maturity of the security services being documented. In some cases, these documents may contain only known requirements, common controls, and templates.
c. Filling in these documents should begin as early as possible during the project.
d. These documents will need to be updated toward the end of user acceptance testing to ensure that they are accurate.
e. Security operations should not be driven by documentation of compliance but based on system need and described in compliance with security guidance.

vi. Conduct Testing (Developmental, Functional and Security)

a. Systems being developed or undergoing software, hardware, and/or communication modification(s) must be tested and evaluated prior to being implemented.
b. The objective of the test and evaluation process is to validate that the developed system complies with the functional and security requirements.
c. Vulnerability assessments and minimum baseline hardening should be performed for all information systems.
d. Document testing results.

4.3.3 SDLC Phase: Implementation/Assessment

Implementation/Assessment is the third phase of the SDLC. During this phase, the system will be installed and evaluated in the organization's operational environment. Key security activities for this phase include:

- Integrate the information system into its environment;
- Plan and conduct system certification activities in synchronization with testing of security controls; and
- Complete Go-Live related activities.

i. Create a detailed plan for Go-Live

ii. Assess System Security

a. Systems being developed or undergoing software, hardware, and/or communication modification(s) must be formally assessed prior to being granted formal accreditation.

b. The objective of the security assessment process is to validate that the system complies with the functional and security requirements and will operate within an acceptable level of residual security risk.

iii. Authorize the Information System

a. Ncell should do security authorization of an information system to process, store, or transmit information.

b. This authorization (also known as security accreditation), granted by a senior official, is based on the verified effectiveness of security controls to some agreed- upon level of assurance and an identified residual risk to Ncell's assets or operations (including mission, function, image, or reputation).

c. The security authorization decision is a risk-based decision that depends heavily, but not exclusively, on the security testing and evaluation results produced during the security control verification process. An authorizing official relies primarily on:

I. the completed system security plan;

II. the security test and evaluation results; and

III. the POA&M for reducing or eliminating information system vulnerabilities, in making the security authorization decision to permit operation of the information system and to accept explicitly the residual risk to Ncell assets or operations.

4.3.4 SDLC Phase: Operations and Maintenance

Operations and Maintenance is the fourth phase of the SDLC. In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated. The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient. Operations continue if the system can be effectively adapted to respond to an organization's needs while maintaining an agreed-upon risk level. When necessary modifications or changes are identified, the system may re-enter a previous phase of the SDLC. Key security activities for this phase include:

- Conduct an operational readiness review;
- Manage the configuration of the system;
- Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls; and
- Perform reauthorization as required

i. Review of Operational Readiness

a. Many times, when a system transitions to a production environment, unplanned modifications to the system occur.

b. If changes are significant, a modified test of security controls, such as configurations, may be needed to ensure the integrity of the security controls.

c. This step is not always needed; however, it should be considered to help mitigate risk and efficiently address last-minute surprises.

d. Should a last-minute change occur that fundamentally changes the level of risk to the system, the system owner should consider recertification

ii. Perform Configuration Management and Control

Further changes in the information systems shall be in accordance with the Ncell's Change Management Procedure. Please refer the Change Management Procedure for more information.

iii. Conduct Continuous Monitoring

a. The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways, including security reviews, self-assessments, configuration management, antivirus management, patch management, security testing and evaluation, or audits.

b. Automation should be leveraged where possible to reduce level of effort and ensure repeatability.

4.3.5 SDLC Phase: Disposal

Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place. Information security issues associated with information and system disposal should be addressed explicitly. When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that government resources and assets are protected.

Usually, there is no definitive end to a system. Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System security plans should continually evolve with the system. Much of the environmental, management, and operational information should still be relevant and useful in developing the security plan for the follow-on system.

The disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.
Key security activities for this phase include:

- Build and Execute a Disposal/Transition Plan;
- Archive of critical information;
- Sanitization of media; and
- Disposal of hardware and software.

i. Build and Execute a Disposal/Transition Plan
ii. Ensure Information Preservation
iii. Sanitize Media
Please refer to the Media Handling Procedure for more information on media disposal.

5. Governance and Compliance

i. Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.

6. Associated Documents

i. Information Security Policy
ii. Media Handling Procedure
iii. Information Classification Procedure
iv. Change Management Procedure