Third-Party Risk Management Procedure

Ncell

Procedure

Approved Date:- 13/12/2019

Procedure Name DOCID: PR-IT-IS-09

Document Control

i. Document Identification

Document Title and Version:	**PR-IT-IS-09 Third Party Risk Management Procedure v1.0**
Effective Date:	05-10-2019
Document Author:	Information Security Team
Owner:	Information Security Team

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	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	28-09-2023	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
	Third Party Risk Management Procedure	Owner: Information Security Team
		Effective Date: 05-10-2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO: Andy Chong

Table of Contents

1. Purpose

The Third-Party Management Procedure shall enable Ncell to ensure effective management of its third-party services and mitigate security risks associated with third-party suppliers. The objective of this procedure is to:

i. Identify and categorize Third parties.
ii. Identify the information security requirements from each category of Third party.
iii. Assess the information security readiness for all Third parties; and
iv. Monitor the Third-party performance to ensure adherence of services as per contractual agreements.

2. Review and Updating

This procedure shall be reviewed once every two years or whenever significant changes occur in the organization.

3. Scope

The scope of this procedure is applicable to all Third-parties providing services to Ncell. For the purposes of this document, a ‘Third-party’ is one who associates with Ncell and is involved in handling, managing, storing, processing and transmitting information of Ncell. This definition also includes all sub-contractors, consultants and/or representatives of the Third-party.

4. Roles and Responsibilities

It is the responsibility of every Third-party and their employees, who handle, process, manage and/ or store information of Ncell to understand and adhere to the requirements of this procedure.
Additionally, following are the responsibilities of the various roles/ teams involved in ensuring third party management

4.1 Chief Information Officer

i. Overall accountability to ensure that the Third-Party Risk Management procedure is followed properly.
ii. Provide approval on Third Party Risk Management Procedure and any subsequent modifications; and
iii. Accountable to ensure that Information Security readiness is evaluated for all Third parties as per the defined frequency.

4.2 Information Security Management Representative (IS MR)

i. Ensure that the Third-Party Risk Management Procedure is updated and reflects the requirements of Ncell.
ii. Roll out of the Standard Operating Procedure to heads of all units/ departments for implementation; and
iii. To monitor third party risk management procedure implementation at vendors/ partners associated with Ncell.

4.3 Ncell’s Third Party SPOC/ Project Manager

i. Classify all third parties as per the defined service classification.
ii. Ensure the inclusion of all relevant security checklists in the contract as per the identified service classification.
iii. Review the third party’s compliance against the applicable security checklists as per the defined review frequency; and
iv. Initiate an on-site Information Security readiness assessment on the third party as per the defined frequency with the help of Internal Audit team or an independent Third-Party auditor (as appropriate).
v. Ensure that a Non-Disclosure Agreement (NDA) is signed with the Third-party upon the initiation of the project; and
vi. Assign a Project Manager from the team for directly interacting with and monitoring information security requirements from Third-party; and

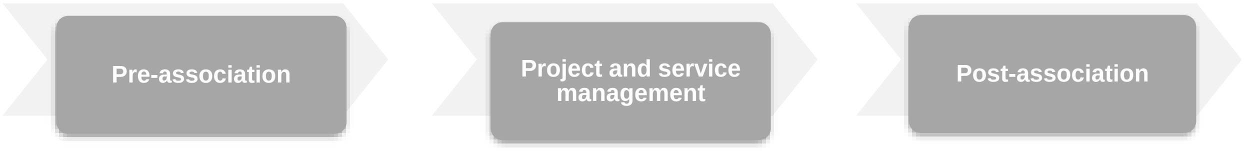
vii. Information security requirements can be monitored through Self-Assessment or onsite reviews.
viii. Define and include the Service Level Agreements (SLAs) and/or Project Milestones with all third parties in consultation with the respective Project Team in the contract.
ix. Ensure that the contract, along with the relevant SLAs/Project Milestones and Security requirements is agreed and formally signed by the third party.

4.4 Third Party

i. Understand, agree and adhere to the security requirements identified as part of the Pre-Association and Post-Association Security Compliance checklists in their day-to-day operation at Ncell;
ii. Ensure that the information security responsibilities are communicated to employees of Third-party providing services to Ncell;
iii. Create performance reports covering the various parameters relating to the defined SLA's and their related compliance; and
iv. Extend support to the respective operations/ project team in conducting onsite reviews/self-assessments against the security checklists.

5. Third Party Management Process

The business model of Ncell largely depends on its third parties. Therefore, it is essential to ensure that services from the third parties are regularly reviewed for security requirements and availability as per the agreed Service Level Agreements (SLA) and scope of work. To ensure the same, Ncell has a process of ensuring security management of third party services across the following stages of their association with Ncell:



5.1. Pre-Association Phase

This phase is initiated by release of an RFQ to various third parties. The objective of this phase is to categorize the third-party services, determine the appropriate security controls required to be implemented by third party in relation to delivery of services to Ncell, obtain adherence declaration from the third party against the security requirements and enforce the same through incorporation in business agreements.

5.1.1. Service Categorization Criteria

Service rendered by the third parties could be of the following types: -

i. **UNN** – ***U**ser access on **N**cell's Information System in **N**cell premises*

These include all Third parties who only have access to Ncell's applications and IT/Telecom network and are operating out of Ncell premises. They do not have remote access or admin access to any application and IT/Telecom network. They do not have any physical access (user/ad to Ncell's applications and IT/Telecom network for supporting Ncell's process' and operation

ii. **UNT** – ***U**ser access to **N**cell's Information Systems from **T**hird-party's premises*

These include all Third parties who have user access to Ncell's applications and IT/Telecom network from their own premises or any other premises out of Ncell's premises. They have remote access but not admin access to any application and IT/Telecom network. They do not have any physical access (user/ad to Ncell's applications and IT/Telecom network for supporting Ncell's process' and operation

iii. **ANN** – ***A****dmin access to* ***N****cell's Information Systems in* ***N****cell's premises*

These include all Third parties who have admin access to and are managing Ncell's applications and IT/Telecom network out of Ncell premises. They do not have remote access to Ncell's application and IT/Telecom network. The applications and/or IT/Telecom network managed by these Third parties must be located inside Ncell premises.

iv. **ANT** – ***A****dmin access to* ***N****cell's Information Systems from* ***T****hird-party's premises*

These include all Third parties who have admin access to *Ncell's* applications and IT/Telecom network from their own premises or any other premises out of *Ncell's* premises. They have remote access to *Ncell's* applications and IT/Telecom network. They do not have any physical access (user/ad to *Ncell's* applications and IT/Telecom network for supporting *Ncell's* process' and operation. The applications and/or IT/Telecom network managed by these Third parties must be located inside Ncell premises.

v. **ATT** – ***A****dmin access to* ***T****hird-party's information systems from* ***T****hird-party's premises*

These include all Third parties who manage the applications and/or IT/ telecom Network from their own premises or any other premises out of *Ncell's* premises. The applications and IT/ Telecom network managed accessed by these Third parties are not located within *Ncell's* premises.

vi. **PNN** – ***P****hysical access to* ***N****cell's Information/ information systems from* ***N****cell's premises*

These include all Third parties who only have physical access to *Ncell's* information/ information systems and are operating out of *Ncell's* premises. They do not have any logical access (user/ad to *Ncell's* applications and IT/Telecom network for supporting *Ncell's* process' and operation. The applications and IT/ Telecom network physically accessed by these Third parties are located within *Ncell's* premises.

vii. **PNT** – ***P****hysical access to* ***N****cell's information/ information systems from* ***T****hird-party's premises*

These include all Third parties who only have physical access to *Ncell's* information/ information systems and are operating out of their own premises or any other premises out of *Ncell's* premises. They do not have any logical access to *Ncell's* applications and IT/Telecom network for supporting *Ncell's* process' and operation. The applications and IT/ Telecom network physically accessed by these Third parties are located outside *Ncell's* premises.

		UNN	UNT	ANN	ATT	ANT	PNN	PNT
Type of access granted	Admin Access			√	√	√		
	User Access	√	√					
	Physical Access						√	√
Location of work	Ncell's premises	√		√			√	
	3rd party premises		√		√	√		√
Location of IT/ Network systems	Ncell premises	√	√	√		√	√	√
	3rd party premises/ any location outside Ncell				√			

5.1.2. Security Controls Applicability Matrix

Based on the service classification, relevant information security controls from ISO 27001:2013, shall be determined as per the following matrix:

ISO 27001:2013 Domain	Control	UNN	UNT	ANN	ANT	ATT	PNN	PNT
Organization of information security	Information security roles and responsibilities	×	×	×	×	×	×	×
	Segregation of duties	×	×	×	√	√	×	×
	Contact with authorities	×	×	×	×	√	×	√
	Contact with special interest groups	×	×	×	×	×	×	×
	Information security in project management	×	×	×	×	×	×	×
	Mobile device policy	×	√	×	√	√	×	×
	Teleworking	×	×	×	×	√	×	×
Human resource security	Screening	√	√	√	√	√	√	√
	Terms and conditions of employment	×	×	×	×	×	×	×
	Management responsibilities	×	×	×	×	×	×	×
	Information security awareness, education and training	√	√	√	√	√	√	√
	Disciplinary process	√	√	√	√	√	√	√
	Termination or change of employment responsibilities	√	√	√	√	√	√	√
Asset management	Inventory of assets	√	√	√	√	√	√	√
	Ownership of assets	√	√	√	√	√	√	√
	Acceptable use of assets	√	√	√	√	√	√	√
	Return of assets	√	√	√	√	√	√	√
	Classification of information	√	√	√	√	√	√	√
	Labelling of information	√	√	√	√	√	√	√
	Handling of assets	√	×	√	×	√	√	√
	Management of removable media	×	√	×	√	√	×	×
	Disposal of media	×	√	√	√	√	×	√
	Physical media transfer	×	√	×	√	√	×	√
Access control	Access control policy	×	×	√	√	√	×	√
	Access to networks and network services	×	×	√	√	√	×	×
	User registration and de-registration	×	×	√	√	√	×	×
	User access provisioning	×	×	√	√	√	×	×
	Management of privileged access rights	×	×	√	√	√	×	×
	Management of secret authentication information of users	×	×	√	√	√	×	×
	Review of user access rights	×	×	√	√	√	×	√
	Removal or adjustment of access rights	×	×	√	√	√	×	×
	Use of secret authentication information	√	√	√	√	√	×	×

ISO 27001:2013 Domain	Control	UNN	UNT	ANN	ANT	ATT	PNN	PNT
	Information access restriction	×	×	√	√	√	×	×
	Secure log-on procedures	×	×	√	√	√	×	×
	Password management system	×	×	√	√	√	×	×
	Use of privileged utility programs	×	×	√	√	√	×	×
	Access control to program source code	×	×	√	√	√	×	×
Cryptography	Policy on the use of cryptographic controls	×	√	√	√	√	×	×
	Key management	×	√	√	√	√	×	×
Physical and environmental security	Physical security perimeter	×	√	×	√	√	√	√
	Physical entry controls	×	√	×	√	√	√	√
	Securing offices, rooms and facilities	×	×	×	×	×	√	×
	Protecting against external and environmental threats	×	√	×	√	√	×	√
	Working in secure areas	×	×	×	×	×	√	×
	Delivery and loading areas	×	×	×	×	√	√	√
	Equipment siting and protection	×	×	×	×	√	√	×
	Supporting utilities	×	×	×	×	√	√	×
	Cabling security	×	×	×	×	√	√	×
	Equipment maintenance	×	×	×	×	√	√	×
	Removal of assets	×	√	×	√	√	×	×
	Security of equipment and assets off-premises	×	√	×	√	√	×	×
	Secure disposal or reuse of equipment	×	√	×	√	√	√	×
	Unattended user equipment	×	√	×	√	√	√	×
	Clear desk and clear screen policy	×	√	×	√	√	√	√
Operations security	Documented operating procedures	√	√	√	√	√	√	√
	Change management	√	√	√	√	√	×	×
	Capacity management	×	×	×	√	√	×	×
	Separation of development, testing and operational environments	×	×	×	√	√	×	×
	Controls against malware`	×	√	×	√	√	×	×
	Information backup	×	√	√	√	√	×	×
	Event logging	×	×	√	√	√	×	×
	Protection of log information	×	×	×	√	√	×	×
	Administrator and operator logs	×	×	√	√	√	×	×
	Clock synchronization	×	×	√	√	√	×	×

ISO 27001:2013 Domain	Control	UNN	UNT	ANN	ANT	ATT	PNN	PNT
	Installation of software on operational systems	×	×	√	√	√	×	×
	Management of technical vulnerabilities	×	×	√	√	√	×	×
	Restrictions on software installation	×	√	√	√	√	×	×
	Information systems audit controls	×	×	×	×	√	×	×
Communications security	Network controls	×	×	×	×	√	×	×
	Security of network services	×	×	×	×	√	×	×
	Segregation in networks	×	×	×	×	√	×	×
	Information transfer policies and procedures	×	×	×	×	√	×	×
	Agreements on information transfer	×	×	×	√	√	×	×
	Electronic messaging	×	×	√	√	√	×	×
	Confidentiality or nondisclosure agreements	√	√	√	√	√	√	√
System acquisition, development and maintenance	Information security requirements analysis and specification	×	×	√	√	√	×	×
	Securing application services on public networks	×	×	√	√	√	×	×
	Protecting application services transactions	×	×	√	√	√	×	×
	Secure development policy	×	×	√	√	√	×	×
	System change control procedures	×	×	√	√	√	×	×
	Technical review of applications after operating platform changes	×	×	√	√	√	×	×
	Restrictions on changes to software packages	×	×	√	√	√	×	×
	Secure system engineering principles	×	×	√	√	√	×	×
	Secure development environment	×	×	√	√	√	×	×
	Outsourced development	×	×	×	√	√	×	×
	System security testing	×	×	√	√	√	×	×
	System acceptance testing	×	×	×	√	√	×	×
	Protection of test data	×	×	√	√	√	×	×
Supplier relationships	Information security policy for supplier relationships	×	√	×	√	√	×	√
	Addressing security within supplier agreements	×	√	×	√	√	×	√
	Information and communication	×	×	×	√	√	×	×

ISO 27001:2013 Domain	Control	UNN	UNT	ANN	ANT	ATT	PNN	PNT
	technology supply chain							
	Monitoring and review of supplier services	×	√	×	√	√	×	√
	Managing changes to supplier services	×	√	×	√	√	×	√
Information security incident management	Responsibilities and procedures	×	×	×	×	√	×	√
	Reporting information security events	√	√	√	√	√	√	√
	Reporting information security weaknesses	√	√	√	√	√	√	√
	Assessment of and decision on information security events	×	×	×	×	√	×	√
	Response to information security incidents	×	×	×	×	√	×	√
	Learning from information security incidents	×	×	×	×	√	×	√
	Collection of evidence	×	√	×	√	√	×	√
Information security aspects of business continuity management	Planning information security continuity	×	×	×	×	√	×	√
	Implementing information security continuity	×	×	×	×	√	×	√
	Verify, review and evaluate information security continuity	×	×	×	×	√	×	√
	Availability of information processing facilities	×	×	×	×	√	×	×
Compliance	Identification of applicable legislation and contractual requirements	√	√	√	√	√	√	√
	Intellectual property rights	√	√	√	√	√	√	√
	Protection of records	√	√	√	√	√	√	√
	Privacy and protection of personally identifiable information	√	√	√	√	√	√	√
	Regulation of cryptographic controls	×	√	×	√	√	×	×
	Independent review of information security	×	√	×	√	√	×	×
	Compliance with security policies and standards	√	√	√	√	×	√	√
	Technical compliance review	×	×	×	√	√	×	×

Legend	
√	Applicable
×	Not Applicable

The security requirements, as determined in the above matrix, shall be applicable before and after association with the third parties. Accordingly, the following types of checklists shall be formulated by Ncell:

i. <u>Pre-association checklist</u>

The *Pre-Association Security Compliance Checklist* defines the security requirements of Ncell. This checklist shall be distributed to the third parties of Ncell to declare the controls they adhere to. The checklist is defined into two categories of controls – Critical and Major. Compliance to the critical information security controls is mandatory for the third parties.
[Refer Annexure A: S. No. 1: Pre-Association checklist]

ii. <u>Post-association checklist</u>

The *Post-Association Security Compliance Checklist* provides guidance to ensure third party's compliance against Ncell's security requirements and the controls that they have put in place to maintain the same, after their association with Ncell.
[Refer Annexure A: S.No. 2: Post-Association checklist]

5.1.3. Preliminary Compliance Assessment

i. Post determination of the security requirements expected from the Third-party, Ncell's SPOC/Project Manager shall communicate the Pre-Association checklist to the Third-party.

ii. In response to this, the Third-party shall perform a preliminary self-assessment on the security controls and report their compliance status (Complied/ Not Complied/ Not Applicable) to the Ncell's SPOC/Project Manager; and

iii. The compliance scores shall be shared by the Ncell's SPOC/Project Manager with Information Security team. These scores shall enable Ncell in selecting an appropriate party for providing services to the organization.

iv. **<u>Evaluation Criteria:</u>**

100% compliance to the 'Critical' information security controls is mandatory for the third parties. In addition, at-least 60% compliance score is required against the 'Major' category of information security controls.

5.1.4. Inclusion of security requirements in supplier agreements

i. Post selection and finalization of the Third-party, the Pre and Post Association Security Compliance checklists shall be included in the Business Agreements for ensuring information security throughout the project lifecycle. These security requirements shall also be applicable on the sub-contractors of the third party (as applicable).

Following are the detailed action steps with respect to the pre-association phase along-with the responsibilities of key personnel:

No	Activity	Responsibility	Documents Required	Processing Time
Pre-Association phase				
1.	Initiate association with third party by communicating the required services to the Procurement Team	Ncell's third party SPOC	NA	NA
2.	Categorize the third party services	Project Manager	Service categorization criteria	NA
3.	Determine the appropriate security controls applicable on the third party in the form of a Pre-Association checklist and Post-association checklist	Project Manager	Security controls applicability matrix	NA

No	Activity	Responsibility	Documents Required	Processing Time
4.	Communicate the security checklists to the Third party	Procurement Team	Pre-Association checklist and Post-association checklist	NA
5.	Perform a preliminary self-assessment on the security controls and report adherence to the Project Manager/Ncell SPOC	Third party	Pre-Association checklist and Post-association checklist	NA
6.	Evaluate the scores of the third party as per the inputs provided by them	Information Security Team	Pre-Association checklist and Post-association checklist	NA
7.	Select an appropriate third party, taking into consideration the adherence status against Ncell’s security requirements	Procurement Team	Technical/ Commercial/ Information Security controls	NA
8.	Define Service Level Agreements (SLAs) pertaining to the third-party services	Project Manager	NA	NA
9.	Include the SLAs and Pre/ Post-Association checklists in the Business Agreements for ensuring information security throughout the project lifecycle	Procurement Team	Project SLAs Pre-Association checklist and Post-association checklist	NA

5.2. Project and service management

This phase involves regular security reviews and service monitoring throughout the project/service lifecycle. This is an ongoing activity that is in advance planned and timely executed to ensure the systematic functioning of the process and review mechanism.

5.2.1. Security Reviews

Security reviews against the information security requirements shall be conducted on an annual basis. Following are the mechanisms of conducting the security reviews:

i. ***Self-assessment***: The third party is required to report compliance status against the security requirements as defined in the pre-association checklist at least on an annual basis.

ii. ***On-site assessment***: Depending upon the criticality of services, on-site assessment may be conducted by either Ncell’s Internal Audit team or by a Third-Party auditor hired by Ncell. During this activity, the third parties must readily provide complete support for the review process.

5.2.2. Service Level Monitoring

A regular monitoring of the service delivery of the third-party shall be done against the agreed service levels. Typically, some of the information, which must be monitored, is:

i. Number of violations with respect to the Service Level agreement.
ii. Reason for violation.
iii. Number of outstanding projects issues.
iv. Time lag for clearing issues.

v. Achievement of the service levels; and
vi. Security breaches of the service contract.

The relationship owners must participate in periodic review meetings with the third party to discuss the performance reports. Service review meeting gives the opportunity to re-look into the performance of the services provided and identify areas/ opportunities of improvement.

5.3. Post Association

This phase is initiated upon concluding the service delivery/ implementation. The official completion of the project will be dependent not only upon the operational closure, but also on security reviews by the respective third-party SPOCs to ensure the following:

i. Compliance SLAs as defined in the contracts.
ii. Verification of deliverable submission.
iii. Update of organizational process assets; and
iv. Closure of administrative and logistical aspects such as archival of documentation and return of physical assets issued during the project initiation phase.

A post-association checklist shall enable Ncell to ensure that all information security risks associated during/ and post project closure stage are identified and treated before dissociating with the third party.

Following are the detailed action steps with respect to the project management phase along-with the responsibilities of key personnel:

No.	Activity	Responsibility	Documents required	Processin g Time
1.	Initiate project closure as per the project deadline defined in the contract	Ncell's third party SPOC	NA	NA
2.	Roll-out of the post-association checklist to the third party	Ncell's third party SPOC	Post association checklist	NA
3.	Follow-up with the third party for initiation of closure actions defined in the checklist	Ncell's third party SPOC	NA	NA
4.	Report closure status with respect to the action items defined in the checklist	Third party	NA	NA
5.	Review closure of the security requirements by the third party	Ncell's third party SPOC & Information Security Team	NA	NA

6. Non – Compliance and Managing Exceptions

The Pre and Post Association checklists are intended to be the statement of information security requirements that need to be met by the third party. Non-compliance with the security requirements and/ or agreed SLA's shall be dealt with consequences as defined in the business agreement with the third party.

However, in case a third party perceives difficulty in adhering to any of the controls, exceptions for an individual control may be requested by the third party. Exceptions are applicable only if approved by the Information Security Officer.

Following are the detailed action steps with respect to raising exceptions to the Ncell Third Party Security Policy:

No.	Activity	Responsibility	Documents required	Processin g Time
1.	The third-party SPOC shall fill up an exception form for raising exception against third party security controls and forward the same to their respective department head	Third party SPOC	Exception Form	NA
2.	Department head shall review the exception and provide approval considering the information security requirements of Ncell	Department Head	Exception Form	NA

3.	IS Team shall review the exceptions from information security perspective and provide feedback to the ISO	Information Security Team (IS Team)	Exception Form	NA
4.	IS Head shall provide the final sign-off on the raised exception	Information Security Officer (ISO)	Exception Form	NA
5.	IS Team shall communicate the approved/ rejected status of the raised exception to the relevant stakeholders	IS Team	NA	NA

7. Associated Documents

i. Information Security Policy
ii. Incident Management Procedure.
iii. Acceptable Usage Guidelines

Annexure A

S. No.	Template Description	Template
1.	Pre- Association Checklist	Pre-Association Checklist A.xlsx
2.	Post Association Checklist	Post-Association Checklist A.xlsx