HR Security Procedure

Ncell

Approved Date:- 06/02/2020

Ncell	Ncell Axiata Limited	Classification: Internal
	HR Security Procedure	Owner: HR Team
		Effective Date: 06-02-2020
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO: Andy Chong

Procedure Name DOCID: IT-IS-PR-2020-12

Document Control

i. Document Identification

Document Title and Version:	**IT-IS-PR-2020-12 HR Security Procedure**
Effective Date:	06-02-2020
Document Author:	Information Security Team
Owner:	HR Team

ii. Distribution List

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

iii. Document Roles and Responsibilities

Responsible	HR Team
Accountable	CHRO
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO	CIO/Head of IT
CHRAO	HR Manager

v. Revision History

Rev	Date	Author	Description	Approved By	Date
0	02-10-2019	Information Security Team	Initial document	Yuvraj Shrivastava	20/12/2019
1	06-02-2020	Tarani Prasad Chaudhary	Revised, Formatting and minor changes for approval	Andy Chong	06-02-2020
2	20-10-2021	Information Security Team	Reviewed with no change	Yuvraj Shrivastava	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	25-04-2024	Information Security Team	Re-branding	CIO/Head of IT	06-06-2024

Table of Contents

1. Purpose

This document sets out Ncell's procedure to minimize risk that staff pose to organizational assets through the malicious use or exploitation of their legitimate access to the organization's resources.

2. Review and Updating

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

3. Scope

This standard 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. Implementation of controls for staff shall be managed by the HR. For vendors, the onus shall lie with the project manager/third party SPOC. 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. Position Risk Designation

Ncell should follow for position risk designations:

i. Assign a risk designation to all positions.
ii. Establish screening criteria for individuals filling those positions.
iii. The risk level associated with each user role that has access to the information system must be assessed.
iv. Position sensitivity levels should be reviewed annually and revised as appropriate.
v. Position risk designations should be reviewed and revised at a minimum, every three years when completed in conjunction with the appraisal process or When a change to or addition of duties occur.

A position's risk designation should consider:

i. Physical access to the information system's hardware or software.
ii. The ability to override or bypass security controls.
iii. The scope of IT resources potentially impacted by security violations

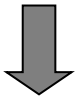
5. Personnel Screening

Personnel screening or employment screening verifies certain data of future and/or existing employees. The process determines if a person is reliable and does not pose a potential risk to the organization.

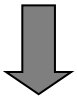
i. Ncell shall:
    a. Screen individuals prior to authorizing access to the information system.
    b. Rescreen individuals as per the organization's requirements.
ii. Personnel screening may be performed by the HR team or a third party hired specifically for the task.
iii. Ncell should define and employ the screening and rescreening criteria and frequency for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.
iv. Ncell should ensure that personnel accessing an information system processing, storing, or transmitting classified information is cleared and indoctrinated to the highest classification level of the information on the system.
v. Ncell shall consider the below minimum while doing the Personnel Screening for a future employee:
    a. *Academic Background:* Part of the internal verification process that covers the school and university that the candidate has attended including degrees obtained and other scholastic records.
    b. *Background Verification:* Verification of correctness of information provided by the employee for his/her academic qualification and professional experience (reference checks).
    c. *Employee File*:Employee file stores information gleaned about each individual candidate as he/she goes through the recruitment/change in role process. These files can be in hard copy form or electronic format or in a combination of these.
    d. *Hiring Manager:* A company officer authorized to initiate the request to hire staff as required by his/her project/department.

vi. Ncell should adhere to the following process, to ensure that all employees undergo thorough background verification.

Candidates shortlisted for hiring



Conduct background verification



Background Verification Result

5.1 Inputs required for background verification

i. Candidates shortlisted for hiring: All shortlisted candidates will act as an input to this process.
ii. Change in business role for existing employee: Employees who transfer into a new role that requires a higher level of background verification clearance can also be an input in this process as per the Department Head's recommendation.

5.2 Outputs generated from background verification

i. Background verification result: The output of this process shall enable the HR department to evaluate individuals' eligibility to be engaged with Ncell. The output shall confirm the authenticity of the data/documents provided and highlight any discrepancy found.

Sr. No.	Activity	Responsibility	Documents Required	Processing Time
Prior to Hiring				
1.	The Hiring Manager should notify HR about shortlisted candidates.	Hiring Manager	NA	NA
2.	Employment Offer is given to employees with the condition of medical test and background verification test	Compensation and Benefits	NA	NA
3.	The HR operations team should ask the shortlisted candidates to provide the below information: • Personal detail • Citizenship Proof or ID • Contact detail: Current Address and Permanent Address • Educational records • Last employment details	HR Resourcing	• Employee form	NA
4.	To ensure the accuracy of the information provided by the candidate, HR Resourcing team or a third party hired for personnel screening should perform the following:	HR Resourcing	• Reference Check Form	2 weeks
	Citizenship/ Identity check: • Obtain a copy of the citizenship ID and PAN card (if available).		• Copy of the citizenship ID and PAN card.	

	Education check: • Obtain a copy of the education certificates - School, Graduation, Masters (if any) etc. • For senior positions, i.e. VP and above, candidates having overseas education may be carried out on case-to-case basis as per management's discretion.		• Copy of the education certificates (School, graduation, post-graduation[if any])	
	Employment check: • Request the shortlisted employee to provide a release letter/ experience letter from the last organization of employment to ensure authenticity of the candidate's last work-experience. • Request the shortlisted employee to provide the last pay slip.		• Release/experience letter from the last organization • Copy of last pay slip	
	Professional reference check: • Conduct an employee database check to ensure that the shortlisted employee is not an ex-Ncell employee with a negative record • For Senior Management Roles (VP and above), Ncell may conduct professional reference check from referred persons in the candidate's previous organization over a call. The feedback obtained shall be documented. • Additionally, for foreign nationals, wherein an employment release letter or experience certificate is not available with the prospective employee due to lack of practice in the country of last employment, professional reference checks should be mandatory. • For scenarios, wherein feedback is not obtained from any provided source, the Resourcing Team may obtain feedback from HR fraternity and peers in the referred organization. In either case, the feedback obtained shall be documented All evidences should be updated and maintained in the employee file.		NA	
5.	HR Resourcing team should update the Hiring Manager about the status	HR Resourcing	NA	NA

	of the verification process conducted. • Passed: Recruitment process can proceed. • Failed/Data not obtained: Discuss with Hiring Manager/ HR Resourcing Head and take appropriate action, as mutually agreed upon.			

6. Personnel Termination

Upon termination of individual employment, Ncell should:

i. Terminate information system access (immediately).
ii. Include exit interviews as it ensures that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property.
    a. Counsel the terminated individual on continued obligations under information system non-disclosure, confidentiality, or user access agreements.
    b. Determine all information systems to which the individual had access and email distribution list memberships.
    c. Ensure there is no DLP (Data Leakage Prevention) incident against the terminated employee in the exit checklist.
iii. For voluntary termination (i.e., normal, scheduled), information system access should be terminated 24 hours within the employee's last working day.
iv. For involuntary termination (i.e., emergency, adverse), information system access should be terminated within four hours of notification of such termination. Disabling of passwords and locking of account should be done on the same day.
v. Retrieve all security-related organizational information system-related property.
vi. Before archiving or permanent disabling of accounts, all the information should be transferred to appropriate personnel or archives.
vii. Retain access to organizational information and information systems formerly controlled by terminated individual.
viii. The following activities should be performed for all personnel, including contractors, leaving, changing jobs, or on extended absences:
    a. Change or cancel all passwords, codes, user IDs, and locks.
    b. Disable user IDs for extended absences (More than 60 days).
    c. Update access control lists, mailing lists.
    d. Collect all keys, badges, and similar items.
    e. Reconcile any financial accounts over which the employee had control.
    f. Ensure electronic records are accessible and properly secured, filled, or appropriately disposed.
ix. Ncell may follow the below for terminated employees:
    a. Notify employees of applicable, legally-binding post-employment requirements for protection of organizational information.
    b. Employ automated mechanisms to notify the employees upon termination of any employee.

7. Access Agreements

Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized.

i. Ncell should ensure that individuals requiring access to organizational information and information systems sign access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements) prior to being granted access.
ii. Ncell should review/update of the access agreements:

a. Annually.
b. Whenever there is a significant change to the information system or information being processed.
c. Whenever there is a change to the agreement.

iii. An individual's current, signed access agreements must be kept on file for one fiscal year after termination.
iv. For access management pertaining to technology and IT systems, please refer to Ncell's User Access Management Procedure.

8. Third-Party Personnel Security

Third-party providers include contractors and other organizations providing information system development, information technology services, outsourced applications, and network and security management to Ncell. Implementation of controls for third party/vendors shall be the responsibility of the respective project managers/third-party SPOC.
Ncell should follow the below minimum for Third-Party Personnel Security:

i. Establish personnel security requirements including security roles and responsibilities for the third-party providers and monitor provider compliance.
ii. Require third-party providers to comply with personnel security procedure of Ncell.
iii. Document personnel security requirements.

Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by Ncell. Third-party should notify Ncell about the personnel changes (transfer or termination) and should ensure appropriate termination of privileges and credentials (immediately).

9. Governance and Compliance

i. Exception management process shall be followed to raise the exception for this procedure.
ii. Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.
iii. Ncell should employ a formal sanctions process for personnel failing to comply with established information security policies and procedures which may include:
    a. Informal corrective actions.
    b. Formal disciplinary actions.
    c. Severe disciplinary actions.
    d. Removal of system access.
    e. Possible criminal and/or civil penalties

10. Associated Documents

i. Access Management Procedure