Access Management Procedure

Ncell

Procedure

Approved Date:- 26/10/2015

Procedure Name DOCID: PR-IT-IS-07

Document Control

i. Document Identification

Document Title and Version:	**PR-IT-IS-07 Access Management Procedure v2.1**
Effective Date:	26-10-2015
Document Author:	Information Security Team
Owner:	Information Security Team

ii. Distribution List

All Ncell Employees
External Auditor (If Required)

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Ncell Employees and External Auditor (If required)

iv. Digital Signature

CEO	CCO	CTO	CIO/Head of IT
CHRAO	CLRCSO	CSO	CFO

v. Revision History

Rev	Date	Author	Description	Approved By	Date
0	26-10-2015	Deepram Mahajan	Initial document	Andras Pali	26-10-2016
1	05-12-2016	Deepram Mahajan	Revised	Simon Perkins	15-12-2016
2	15-08-2019	Information Security Team	Revised – Aligned with current processes	Vishal Mani Upadhyay	13-12-2019
3	01-10-2019	Information Security Team	Revised – Formatted Document	Andy Chong	17-12-2019
4	20-10-2021	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	19-12-2021
5	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
6	23-08-2023	InfoSec Team	Review: changed from Annually to once in every two years 8.4.v account deletion timelines to follow password management guidelines 9.2. iv: changed all criticality from quarterly to quarterly for Min CJ, CJ and yearly for the rest 9.4 MFA requirement added Added Head of IT		
7	30-04-2024	InfoSec Team	Re-branding	CIO/Head of IT	

Table of Contents

1. Purpose

The purpose of this document is to describe the procedure of user creation, deletion, or updating of user account authority in the system. This document lays down the guide-line to be followed during the end-to-end operation in a systematic and schedule manner to ensure completeness, consistency and adherence to timelines.

2. Mission

To enable secure and efficient access to organizational resources through effective identity and access management practices, ensuring confidentiality, integrity, and availability of data while minimizing risks and complying with regulatory requirements.

3. Vision

To establish robost IAM program that empowers employees, partners, and customers with seamless and secure access to resources anytime, anywhere, while maintaining the highest standards of security, privacy, and compliance.

4. Review and Updating

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

5. Scope

This procedure applies to the entire organization and respective external parties who have access to Ncell owned assets and services.

6. Guiding Principles

The following principles shall be considered in the Logical Access Management process, which can be provisioned to maintained using IDAM (IAM / PAM) approved tools and trackers:

i. Logical Access Management related activities shall be documented and reported. This will ensure consistency and traceability in the Logical Access Management process.
ii. Relevant work instructions shall be established and linked to the Logical Access Management process. This will ensure compliance with the Logical Access Management process requirements, enhance efficiency and common ways of working.
iii. All Logical Access requests shall follow the approval structure for the Logical Access Management process. This to ensure that all users with access to systems and services are authorized to access the system and have the correct access rights.
iv. No shared accounts shall be used neither for normal nor for privileged accounts. This will ensure that all accesses to critical data and systems can be monitored and tracked.
v. Accountabilities shall be defined in case of established generic, default / system generated common IDs.
vi. Unit Heads/Section mangers should be accountable for confirming/approving the access to the user.

7. Roles and Responsibilities

7.1 Unit Heads & Above

Shall be responsible for:

i. Evaluating elevated access rights for all Ncell managed applications, databases, servers and tools and send the inputs to function heads for approval,
ii. Evaluating and approving role creation or any role change request related to the Ncell managed applications, databases, servers and tools,
iii. Safeguarding the Administrator Passwords for Ncell managed databases, application, servers & tools,

iv. Identifying privileges and mapping them with job functions to develop and maintain Access Privilege Matrix,

v. Reviewing the application and database access logs and take necessary actions in case of any discrepancy identified, accordingly send the details to function head for final sign-off, and

vi. Reviewing access privilege matrix and send the inputs to function head for approval and take the necessary actions accordingly.

7.2 HR Department / SPOC

i. Shall be responsible to manage organization's onboarding and offboarding process from employee hire to retire,

ii. Shall be responsible to control the transfer cases in the organization,

iii. Shall keep updated the organization chart in the system basis on the role change or modified etc.

7.3 ID / Role / Access Requester

i. Any employee in the organization can raise the request for the privilege or non-privileged accesses and accesses will be granted post authorized evaluation and approvals.

ii. New ID request in the domain shall be initiated by HR and onboarding process shall be followed.

iii. Visitor's / vendor ID and access requests shall be initiated by the respective service teams and authorized by service owners after business need evaluation. Function heads shall be kept informed in such cases. Super admin privileges for vendors shall be approved by function heads.

8. User Access Management

The Logical Access Management process includes three different types of accesses. The type is determined based on the characteristics of the user and the permissions of the requested logical access. The three logical access types are explained in the table below:

Type of access	Access description
Normal	Access to be able perform normal job duties
Privileged	IT administrator access needed systems and services
External	Access to systems and services for customers and vendors

8.1 User account creation and modification

i. When an employee or sub-contractor joins Ncell, the Human Resource (HR) team will create a user in SAP. After the user is created in SAP, the information shared to IT Service Desk and employee's manager. The IT Service Desk will then provide the basic HR service accesses to the employee/user account.

ii. The HR related basic access includes the access to e-mail, office wi-fi, common folder and NGAGE.

iii. There are two types of accesses defined at Ncell, i.e. HR related and technical related. The HR related access will be same for all employees and the technical related basic access will be same for each team. Technical access may differ from team to team and should be defined by Line manager.

iv. After the basic HR access is provided, the employee will request for the basic technical access with his/her manager's approval which will be provided in accordance with the current team's roles. No generic or shared user should be provided the accesses. It is recommended that the user is first given only the test bed access and once the manager feels that the person is competent to handle the production, the manager should request for the access rights for the user.

v. In case of temporary employee, the last date of employment should be filled in Active Directory and the access should be revoked within 24 hours of employee leaving Ncell.

vi. Information for all external person (Name, company name, period for which the username will be required, etc.) should be maintained in external active directory. Ncell contact person will create a request in the identity management system. Once approved, relevant information will be populated in the external AD. Username should reflect if the user is an external one (e.g.: Abc_bijay). For more than one person(s) having the same name, it should be indicated with the numerical number at the last of user name (e.g. Abc_bijay1). External person might have different user ID, based on different contracts. The period of access relating to the different contracts will be different. For internal employee, the business job role will come from HR or Line Manager. For external person, the job role will come from the Ncell contact person.

vii. In case any system or application doesn't support personalized user names and the user must use generic user names for logging in any of the applications, there should be an approval process followed and accountability shall be tagged, so that it can be tracked who is actually using that login for particular changes.

8.2 User's job role changes

The job tasks changes might be due to promotion or transfer to new department or due to some other reasons and HR should change job role(s) in HR SAP. Following process needs to be followed for every job change:

i. Employee needs to request the basic technical access if the accesses are changed. Employee will also request for new accesses in accordance with the current teams and roles.

ii. In case of external person, the information should be changed and maintained in active directory. Ncell contact person will be responsible for updating the job role change of the external person to IT Service Desk, so that he same can be update in AD. Rest of the process will be same as followed for internal person(s).

iii. If the user's manager/contact person makes a request at the same time for "transition period" (max. 1 month) on time (request should be sent 1 week prior the effective date of job role changed, position changed and in case of resignation), the user will still have the old job role for some time without any other approval. In case, the manager doesn't request for "transition period", old job will be taken away and access rights based on that role will be removed while providing the new ones. Change of job roles, positions and resignation should be notified to IT Service Desk at least 5 days prior. This should include the exclusion and inclusion list of email distribution, change in accesses required (new accesses to be provisioned, old ones to be removed), effective date of new role etc.

iv. Additional access rights given to a person (which are not based on job role) will also be removed at this point. In case of Consultant becoming permanent employee in Company, he/she will be treated as a new employee in all applicable systems. Old accesses should be revoked.

8.3 Sabbatical Period (3 months and above)

The final decision for long term absence comes from HR. After the approval from HR, manager needs to decide what accesses will the employee require during his/her absence.

i. If case no access is required, all the access rights will be disabled and de-provisioning process will be started;

ii. If accesses are required, the manager has to confirm which access rights are needed and inform IT Service Desk, HR and security officer. After proper approval from IT, HR and security officer, the required access will be granted and all other access will be revoked;

iii. If a manager takes long term leave, there should be substitute available in HR data (SAP) and manager should give the reference of identified person in his/her auto reply e-mail. In case, there is no fall back defined, HR data will provide manager's senior as a substitute. He/she shall then be responsible for all approvals during that period,

iv. When the employee returns from long term absence, manager should review the access rights required by him/her,

v. Additional access rights will be requested as per the workflow and proper approval process will be followed, and

vi. In case, any employee is not coming to office for more than 3 days without any intimation; the immediate manager should notify the HR and instruct the IT Service Desk which will further send a request to respective admin teams to temporarily block the access. If the employee remains absconded for more than 90 days, the employee's access may be deleted with prior approval from his/her immediate manager.

8.4 User Account Revocation

i. When an employee resigns from Ncell, a notice goes out to direct manager, direct department, all function heads, IT Service Desk/Help Desk, InfoSec, Operations, and Finance departments. The

HR Team shall communicate the details of last working day to the IT Service Desk/Help Desk team. The access to Ncell domain, application, server and tools shall be revoked accordingly by the IT Service Desk team.

ii. Access for sub-contractors shall be revoked automatically based on the last working day captured at the time of access creation; and

iii. In case user access revocation needs to be done immediately, the HR Team shall send the details of the user to IT Service Desk/ Help Desk team through email and the IT Service Desk/Help Desk team shall disable the requested access. Documented information shall be retained for the same by HR team.

iv. In case access revocation of external user needs to be done before the contract expiry date, Ncell contact person can disable the user themselves from the identity management tool or contact IT Service Desk / Help Desk to disable the user.

v. Accounts will be disabled immediately and deleted as per Password Management Guidelines[1] from all the systems that support account deletion. However, in case of some target systems (for example SAP) needs the account still alive in the system, there should be a proper business justification documented for the same and access provisioning team shall make sure that there is no access, whatsoever, associated with that account.

8.5 Access Logs and Rights Reviews

i. All Ncell managed domain IDs, application IDs, system IDs and database Ids shall be reviewed on periodic basis.

ii. User access rights of Crown Jewel (MCJ, CJ) applications will be reviewed at least quarterly

iii. All MCJ, CJ logs (ID and access logs) shall be reviewed/monitored regularly and discrepancies notified to unit head and above and reported to function heads at least on quarterly basis.

iv. Ncell shall provision integration of Crown Jewel (MCJ, CJ) logs with GSOC systems and dashboards shall be published to management in regular reviews.

8.6 Access Matrix

Pre defined and pre-approved list of applications' document.

i. Respective unit heads or above are responsible to identify the different access associated with Ncell managed applications, servers, and tools for their respective teams/units/section.

ii. Based upon the access matrix above, IT and Network team is responsible for developing implementing the approved the Access matrix.

iii. Access matrix shall be managed and reviewed regularly (at least quarterly) by the respective Unit head or above

iv. Access modifications window will be opened for 2 weeks only for Unit heads to update the matrix and after the window is closed, the changes will be implemented by IT and Network team in a bulk.

8.7 General Controls

i. Respective system owners must register their applications in Application Profiles of Process maker, to list all the existing applications. All applications used in Ncell to be recorded in this profile, any application missing in this profile will not get the access as per access matrix or even raised individually.

ii. The Application Profiles to be updated, verified, and approved by respective line managers and system owners.

iii. Any changes in the profiles to be updated or modified regularly by respective system owners.

iv. User based network access to (employees, vendors) to be authenticated via Active directory (AD)

v. UH to update the Access matrix, when the access to be given in bulk.

vi. If individual needs the network access which cannot be put in group based access matrix, it should be raised via process maker and reviewed (1 year maximum) as per end date by respective line manager.

vii. Birth right access will be granted by default to all Ncell Employees (Annex 1.1)

[1] GD-IT-IS-01 Password Management Guidelines

9. Privileged Access Management

Privileged accounts provide elevated, often unrestricted access to an organization's underlying information systems and technology, making them rich targets for both external and internal malicious actors. Often referred to as the "keys to the kingdom," these accounts have been used in successful attacks to gain access to corporate resources and critical systems (e.g., "crown jewels"), resulting in data breaches. All privilege accounts may get secured by PAM (Privilege Access Management) System and managed by Ncell's IT Internal Team. Organization will have the following benefits and focus in line with the privilege access management procedure:

i. Identify vulnerabilities and risk factors within your organization,
ii. limit opportunity for a successful attack by improving control over privileged accounts,
iii. improve efficiencies by reducing the complexity associated with managing privileged accounts, and
iv. simplify compliance by producing automated reports and documentation.

This is the accountability of Head of IT and responsibility of Security and ESPP Head to ensure that privilege access management process is enforced, managed, reviewed and controlled in the organization. Function heads are responsible to ensure that all privilege accounts are managed, maintained and controlled through PAM solution for their respective functional assets.

9.1 Least Privilege Principles

Ncell IT / Technology teams provides accesses basis on the least privilege access principles including the following. Privilege accounts are referred as administrator and root IDs of the assets.

i. All servers shall be under the ownership of OS/Database Planning and Management Team in ESPP. Provision of privilege account follows the principle of least privilege.
ii. Application/service owners are responsible to provision and manage the privilege account in respective apps and databases to follow the principle of least privilege.
iii. Telecom (Transmission systems) and network teams are responsible to provision and manage the privilege account in respective apps and databases to follow the principle of least privilege.
iv. Least privilege principle may get implement in following ways –

   a. Deploy role-based access controls and group policies to prevent employees from accessing information or services that are not required for their job.
   b. Segment the network into VLANs defined by business units to prevent users from freely traversing the network.
   c. Ensure that employees in administrator roles have separate, unique accounts for their administrator and non-administrator activities (i.e., using "Run as Administrator" on pre-approved tasks only).
   d. Perform regular audits of employee accounts to identify changes in roles and prevent privilege creep and former employees from having unauthorized access.
   e. Patch software regularly to reduce the likelihood that end users can exploit software bugs that allow escalation of privilege.

9.2 Access Privilege Matrix

i. Service owners / unit heads & above are responsible to identify the different privileges associated with Ncell managed applications, servers and tools.
ii. These privileges shall be mapped with the job functions to develop and document the access privilege matrix by the respective functions.
iii. Access matrix shall be updated regularly when there is a change (addition / modification / deletion) of any privileged ID or defined role
iv. Access matrix shall be managed (in a form of a document or in PAM tool) and reviewed regularly (at least quarterly for Min CJ, CJ and yearly for the rest) by the respective service owners / Unit head & above and approved by function heads.

9.3 Separation of Duties

Separation of duties metrics for production systems must be implemented to prevent conflict of activities performed by users. The implemented separation of duties along with access privilege metrics shall be documented for future references.

9.4 Multi Factor Authentication

i. Multi factor authentication shall be implemented for access to crown jewels via supported systems, e.g.: Privilege Access Management Tool.
ii. Multi factor authentication shall be implemented for access to email from mobile devices or via web-based access.
iii. Multi factor authentication shall be implemented for access from outside Ncell environment to Ncell devices as per Remote Access Management Guideline[2], e.g.: VPN
iv. Multi factor authentication shall be implemented for admin portals for Ncell services, if accessible from the internet.
v. Multi factor authentication shall be implemented for all portals used for employee services which are accessible from the internet.

10. General Controls

i. All logical access requests activities should be documented.
ii. Identity based accesses, role-based accesses or attribute-based accesses can be provisioned to the users and shall be documented in the access list / metrices.
iii. Administrator/privilege user should only be used for administrative activities and should not be used for regular business activities.
iv. Use of Administrator/privilege access should be consistent with an individual's role or job responsibilities as prescribed by management. When an individual's role or job responsibilities change, Administrator/Privilege Access should be appropriately updated or removed.
v. Service / application accounts should be tagged with the service/application owners to define the accountability.
vi. Account expiry duration should be defined, tracked and reviewed for temporary ID’s.
vii. Use of shared ID’s is prohibited in Ncell IT / Tech system management.
viii. Ncell security team discouraged to use OEM default privilege accounts. In case of any system / tool limitations, exception management process shall be followed and access matrices shall be updated and maintained accordingly.
ix. ID and access reviews shall be conducted for all normal, admin and privilege accounts by respective teams on regular basis.
x. Remote / external users should connect the Ncell network via VPN connectivity.
xi. ID access and activity logs should be maintained as per Ncell log management standard.
xii. Physical and environmental management standard shall be followed for the physical access controls.
xiii. Ncell Password Management Guidelines[3] should be followed, and all administrative / root passwords should be kept securely (prevent from unauthorized access and use) and maintained by respective service owners / Unit Heads & above. They need to ensure that these credentials should be workable during crisis management or disaster scenarios. These critical credentials can be stored in print / electronic forms followed by the key management standards.
xiv. Release of critical passwords –
xv. The owner/custodian of the stored critical passwords shall only release the password to the following persons under the following circumstances: -

Password released to	Circumstance / Reason	Authorization Requirement
Password Owner (Service owner)	On request where: -	None

[2] GD-IT-IS-09 Remote Access Management Guideline

[3] GD-IT-IS-01 Password Management Guideline

Password released to	Circumstance / Reason	Authorization Requirement
	• The password requires changing or replacing. • The owner has forgotten the password. • In case of a firefighting situation.	
Functional Head	The owner of the password has become unavailable to the company (E.g. Termination of service, resignation, death etc. or other emergency)	IT Service Desk / Help Desk

xvi. The custodian of the stored critical passwords shall release the password only upon formal written request over email and upon completion of the following steps: -

a. The release of a password should be noted in a log,

b. Once opened, the password should be considered as ‘compromised’ and should be changed, and

c. The changed password shall be stored again following the same procedure.

11. 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. Compliance to the group’s Access Control Standard and Identification & Authentication Standard in addition to these guidelines is mandatory.

iv. IAM SPOCs should undertake the IAM courses. Example: online LinkedIn courses or any other relevant course to upskill the knowledge on IAM/IDM

v. The risk should be reported in ISC if any.

12. Associated Documents

i. Information Security Policy

ii. SP 800-53 Rev. 4, Security Controls and Assessment Procedures for Federal Information Systems and Organizations. https://nvd.nist.gov/800-53/Rev4/family/Access%20Control

iii. NIST Special Publication 800-53 Rev.4 *https://nvd.nist.gov/800-53*