


Privileged Access Management Procedure

Ncell

Procedure

Approved Date:- 01/10/2019

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Procedure Name DOCID: PR-IT-IS-17

Copyright © Ncell. All rights reserved.

No part of this document may be reproduced or transferred in any form or by any means without prior permission in writing from Ncell.

These trademarks are the intellectual property of Ncell and are protected by applicable legislation.

All other products or company names are used for reference only and may be proprietary to their respective hold

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Document Control

i. Document Identification

Document Title and Version:	PR-IT-IS- 17 Privileged Access Management Procedure v1.0
Effective Date:	1 st October, 2019
Document Author:	Information Security Team
Owner:	CIO/Head of IT














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

			
			CIO/Head of IT
			
CHRAO	RCSO		

v. Revision History

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Rev	Date	Author	Description	Approved By	Date
0	01-10-2019	Information Security Team	Initial document	CEO	01-10-2019
2	05-11-2021	Information Security Team	6.5.iii and 7.iv Added "for Crown jewels"	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 period added. Added Head of IT		
5	30-04-2024	Information Security	Re-branding	CIO/Head of IT	


	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Table of Contents


.....	1
Document Control	3
1. Introduction.....	6
2. Scope	7
3. Principles.....	7
4. Definitions.....	7
4.1. Privileged accounts	7
4.2. Privileged access management (PAM)	8
4.3. Identity Management System (IDM)	8
5. Privilege access management	8
6. Least Privilege	9
6.1. Authorize Access to Security Functions.....	9
6.2. Non-Privileged Access for Non-Security Functions	9
6.3. Network Access to Privileged Commands	9
6.4. Separate Processing Domains.....	9
6.5. Review of User Privileges	9
6.6. Privilege Levels for Code Execution	9
6.7. Auditing Use of Privileged Functions	10
7. Access Privilege Matrix	10
8. Separation of Duties.....	10
9. Process for privilege access request.	10
9.1. Ncell Staff.....	10
9.2. Vendors	10
10. PAM Guidelines	11
10.1. New Device and privileged account integration request.....	11
10.2. Account onboarding process.....	11
10.3. RACI Matrix:	12
10.4. Login Methods.....	13
10.5. Session Recording	13
10.7 System access procedure.....	14
10.8 Emergency cases.....	14
10.8.1 PAM is not accessible	14
10.8.2 PAM is up but the end device is not accessible	14
10.8.3 Device owner not available for L3 account approval	14
10.9 Password rotation	14
10.10 Account discovery	14
10.11 Roles Responsibility matrix	14
11 Exceptions.....	15

Ncell	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

12	References	15
	Annexure – I	15
	System Admin / owner	15
	PAM Admin	16
	Password Custodian	16
	Security Team	16
	Crisis Scenario	16

1. Introduction

The Privileged Access Management process grants authorized users and administrators in professional services rights to use systems and services, while preventing access to non-authorized users. The privileged

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

access management process ensures that only authorized users and administrators get access to services and systems.

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.

The intent of this document is to describe the Privileged Access Management process and related process requirements in Ncell, which aims to support in,

- i. Fulfilment of organization security requirements and increase customer satisfaction.
- ii. Ensuring efficiency and effectiveness in our ways of working
- iii. Managing and mitigating risks

This document does not contain detailed work instructions for specific tasks, requirements and other detailed activities.

2. Scope and Review

This document shall be used as a guiding principle by respective teams in order to meet process requirements and delivery expectations. The document shall be reviewed once every two years or when significant changes occur in the organization.

3. Principles

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

- i. Privileged 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 Privileged Access Management process. This will ensure compliance with the Privileged Access Management process requirements, enhance efficiency and common ways of working.
- iii. All Privileged Access requests shall follow the approval structure for the Privileged Access Management process. This is 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.


4. Definitions

4.1. Privileged accounts

Privileged accounts include local and domain administrative accounts, emergency accounts, application management, and service accounts, which has permission to change user roles, account which has permission to change security and logging configuration of the system/application.

These will typically consist of the following:

- i. Local Administrative Accounts that are non-personal accounts, which provide administrative access to the local host or instance only. Local admin accounts are routinely used by the IT staff to perform maintenance on workstations, servers, network devices, databases, mainframes etc. Often, they have the same password across an entire platform or organization for ease of use. This shared password across hosts makes for a soft target that advanced threats routinely exploit.
- ii. Privileged User Accounts are named credentials which have been granted administrative privileges on one or more systems. This is typically one of the most common forms of privileged account access granted on an enterprise network, allowing users to have administrative rights on, for example, their local desktops or across the systems, they manage. Often these accounts have

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

unique and complex passwords, and the power they wield across managed systems makes it necessary to continuously monitor their use.

- iii. Domain Administrative Accounts have privileged administrative access across all workstations and servers within the domain. These accounts provide the most extensive and robust access across the network. With complete control over all domain controllers and the ability to modify the membership of every administrative account within the domain. A compromise of these credentials is often a worst-case scenario for any organization.
- iv. Emergency Accounts provide unprivileged users with administrative access to secure systems in the case of an emergency and are sometimes referred to as 'fire call' or 'break glass' accounts. While access to these accounts typically requires managerial approval for security reasons. It is usually a manual process that is inefficient and lacks any auditability.
- v. Service Accounts can be privileged local or domain accounts that are used by an application or service to interact with the operating system. In some cases, these service accounts have domain administrative privileges depending on the requirements of the application they are being used for. Local service accounts can interact with a variety of Windows components, which makes coordinating password changes difficult.
- vi. Active Directory or domain service account password changes can be even more challenging as they require coordination across multiple systems. This challenge often leads to a common practice of rarely changing service account passwords, which represents a significant risk across an enterprise.
- vii. Application Accounts are accounts used by applications to access databases, run batch jobs or scripts, or provide access to other applications. These privileged accounts usually have broad access to underlying company information that resides in applications and databases. Passwords for these accounts are often embedded and stored in unencrypted text files, a vulnerability that is replicated across multiple servers to provide greater fault tolerance for applications. This vulnerability represents a significant risk to an organization because the applications often host the exact data that APTs are targeting.

4.2. Privileged access management (PAM)

It refers to a set of processes and tools for controlling, monitoring, and auditing privileged access. Traditional PAM solutions are typically based on password vaults and password rotation.


4.3. Identity Management System (IDM)

IDM refers to a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. IDM systems fall under the overarching umbrella of IT security. Identity and access management systems not only identify, authenticate and authorize individuals who will be utilizing IT resources, but also provision the hardware and applications employees need to access.

5. Privilege 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 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.

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

This is the accountability of CIO and responsibility of Security and IT 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.

6. Least Privilege

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.

- All servers shall be under the ownership of OS/Database Planning Management team in ESPP. Provision of privilege account follows the principle of least privilege.
- Application/service owners are responsible to provision and manage the privilege account in respective apps and databases to follow the principle of least privilege.
- 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.

6.1. Authorize Access to Security Functions

Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

6.2. Non-Privileged Access for Non-Security Functions

Limits exposure when operating from within privileged accounts or roles.

6.3. Network Access to Privileged Commands

Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device, remote access via terminal session, VPN, Telnet, Putty etc.)

6.4. Separate Processing Domains

Providing separate processing domains for finer-grained allocation of user privileges includes, for example:


- Using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine.
- Employing hardware and/or software domain separation mechanisms
- Implementing separate physical domains. (Network management process covering segregation of VLAN requirements etc.)

6.5. Review of User Privileges

- The need of certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environment of operation, technologies, or threat.
- Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.
- Review of user privileged will be conducted on quarterly basis.

6.6. Privilege Levels for Code Execution

- In certain situations, software applications/programs need to execute with elevated privileges to perform required functions.

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- ii. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.
- iii. In such scenarios, the user needs to ensure that the excessive privilege is in line with the allotted role.
- iv. In case, the privilege is associated with a higher role, the user shall request time-based access to execute the code with higher privilege levels.

6.7. Auditing Use of Privileged Functions

- i. Auditing the use of privileged functions is one way to detect misuse of privileged accounts. It even helps to mitigate the risk from insider threats and the advanced persistent threat (APT).
- ii. Admin accounts log review shall be in place and necessary actions shall be taken in case any discrepancies identified.

7. 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) by the respective service owners / Unit head & above and approved by function heads.

8. Separation of Duties

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

9. Process for privilege access request.

9.1. Ncell Staff

Any Ncell employee or contractor require privilege accounts L3 (root ID, admin ID and similar accounts) to any Ncell system must submit a form in JIRA/Identity Management System (IDM). After approval, the user is assigned L3 user via PAM. To use L3 account, the user should fill a request form in PAM. Once the request is approved by device owner, the access would be provided by PAM.

The request in PAM should include below information:


- i. The list of access required. Reason for each access requested.
- ii. Timelines for each privileged access requested (Not exceeding one year).

9.2. Vendors

If a vendor needs privileged account access L3 to Ncell system a form should be submitted in JIRA/IDM by the responsible Ncell Single Points Of Contact (SPOC). After approval, the user is assigned L3 user via PAM. To use L3 account, the user should fill a request form in PAM. Once the request is approved by device owner, the access would be provided by PAM.

The request in PAM must contain:

- i. The list of access required with reason for each access.
- ii. Timelines for each access: it can be in hours or days or maximum 3 months.

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

This procedure is same for all device onboarded in PAM. System owner should check and ensure the usability of account before reassigning the privileged access. User access review will be done as per access management procedure for both Ncell staff and vendors.

10. PAM Guidelines

10.1. New Device and privileged account integration request

Currently CJ devices are only onboarded in PAM however decision to add other devices can be made by IT Security Unit Head and ESPP unit head. When a new device needs to go live in Ncell environment, system owners should fill the necessary Jira workflow (SAR with user access matrix and NAR for access from PAM to end device) with all required details. This template would contain details of server and all privileged accounts. If password of any account should not be rotated, then it should be clearly mentioned on the template and exception form should be filled and approved in SDM. Checklist for new device onboard is in Annex I.

10.2. Account onboarding process

Correlation of users with roles is defined on device and PAM as per below procedure:

- i. Information related to user and role matrix is prepared and uploaded in JIRA-SAR for approval. Sample format can be obtained from IT services team
- ii. User account are created as below. Where applicable, definition of L1, L2 and L3 and root is provided in Table 1.
- iii. Linux/Unix devices: level_1, level_2 and level_3 level users are created on device. What about Nessus.
- iv. Additional to L1, L2 and L3 there is a L4 account which is not managed by PAM. During emergency L4 account comes into effect. Further approval is not required to create these accounts.
- v. Windows devices:
 - a. Windows Server: administrator account should be onboarded in PAM. Administrators should fill PAM form as per described in 9.1 i & ii and 9.2 I & ii.
 - b. Jump host: Named accounts are created as per approved from JIRA/IDM with role L2 as RDP user. Administrator account should be managed as per 10.2 V.a.

Additional to administrator account onboarded in PAM, there is L4 account which is not managed by PAM. During emergency L4 account comes into effect. Further approval is not required to create these accounts.

- iii. Network devices: Domain accounts for Internal users and local accounts for external users/vendors are in TACAS to authenticate in network devices. Roles and permission are managed in TACACS. Separate single domain account is created for internal and external users for login into PAM. Devices are categorised as per network team (like PTN, MBPN & common) and access to these group of devices are provided on bulk after single approval in PAM. Emergency account for each network device is with CTO or team/user authorized by CTO.
- iv. Database: Named account (R, R/W & DBA) for each individual user is created in DB as per approval from JIRA(SAR)/IDM. SYS and SYSTEM accounts will be disabled. There would be Read only and R/W DB accounts.
 - a. Supported Database: These are the database which is supported by PAM for account onboarding and password rotation. OS Level_4 is treated as L4 account in DB. Level_3 account is created in each DB to rotate DB account password. Read only accounts can be used without approval whereas R/W account can be used only after approval in PAM
 - b. Unsupported Database: Account onboard and password rotation for some DBs are not supported by PAM and user accounts cannot be managed by PAM

Ncell	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Users would login to jump via PAM and access both DB (Supported and non supported) via DB client tools. PAM would use (domain/local) RDP users to access jump host. DB account password is retrieved from PAM in case of supported DB and pre-shared password by DBA in case of unsupported DB. R/W

Database access should only be accessed from jump host.

- v. All user accounts mentioned in point ii, are to be created and password is vaulted in PAM.
- vi. For all user accounts vaulted in PAM, password rotation is carried out as per the Ncell password guideline. Direct login via Root user should be disabled on device, in case of Linux and UNIX based devices.
- vii. If there is any special requirement of using application account rather than L1, L2, & L3 then PAM form should be filled with necessary explanation and can be used after switching from 3 account.
- viii. User can see only devices to which they have approved accesses and can only use assigned level of user.
- ix. If any user requires L3 level of access, the approval workflow in PAM will need to be used to request for approval from device owner i.e. Unit Head/Section Manager/PAM administrator/CIO.
- x. Once device is on-boarded and password is vaulted into PAM, privileged accounts are only allowed to log into the end devices via PAM.
- xi. For logging into PAM, user will use their domain credential.

For every device/group of devices, following policy matrix would be set:

Account	User	Remarks
L1	L1 Support	Read only access
L2	L2 Support	Perform daily activities/makes some configuration changes
L3	L3 Support	Like root
L4	Super admin	Super user come in to effect during emergency
Root/administrator	Root/ladm	Root/admin user

10.3. RACI Matrix:

Ncell	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Step	Task	IT Security Team	PAM admin/ESP	IT Services	ESPP- System administrator	End user	Respective Unit Head	Device owner	CIO/CTO
1	Decision to Add device into PAM	A/C	I	I	I	R	R	I	I
2	Open network access from PAM to your system. Source IP [10.18.12.74, 10.18.12.80,10.19.12.74]	I/C	I	A	I	R	I	I	I
3	Create level_1, level_2, level_3, level_4 users	I/C	I	I	R	A	I	I	I
4	Validate level_1 (Read only user)	I/C	I	I	I	R	A	I	I
5	Validate permission of Level_2 [Daily operation account]	I/C	I	I	I	R	A	I	I
6	Validate permission of level_3 [Can switch to root w/o password]	I/C	I	I	I	R	A	I	I
7	Validate level_4 account and its permission.	I/C	I	I	I	R	A	I	I
8	Disable direct root login	I/C	I	I	I	R	A	I	I
9	Disable direct network access in server. Develop use case with GSOC to monitor direct access	I/C	I	I	I	R	A	I	I
10	Prepare Crisis VPN account for break glass scenario.	I/C	I	I	I	R	A	I	I
11	Remove all human account. Strictly use level_1, level_2, level_3 account via PAM only.	I/C	I	I	I	R	A	I	I
12	For using service account, need to take approval of level_3 and switch to root and service account.	I/C	I	I	I	R	A	I	I
13	Prepare or Update Access Matrix of PAM in Jira	I/C	I	I	I	R	A	I	I
14	Review Access Matrix of PAM on quarterly basis	I/C/A	I	R	I	I	A	R	I
15	Prepare policy in PAM as per access matrix table.	I/C	I/A	R	I	I	I	I	I
16	Publish role name in IDM so that user can request access from IDM.	I/C	I/A	R	I	I	I	I	I
17	Set approval flow for level_3.	I/C	I/A	R	I	I	I	I	I
18	Set Black list command filtering.	I/C	I/A	R	I	I	I	I	I
19	Set Session recording	I/C	I/A	R	I	I	I	I	I
20	Send syslog to GSOC	I/C	I/A	R	I	I	I	I	I
21	Rotate password of level_4 as per policy.	I/C	R/A	I	I	I	I	I	R
22	Develop use case to monitor direct login.	R/A/C	I	I	I	I	I	I	I
23	Develop use case to monitor Blacklist command.	R/A/C	I	I	I	I	I	I	I
24	Develop use case to monitor Crisis VPN Login.	R/A/C	I	I	I	I	I	I	I

10.4. Login Methods


All PAM users can login in to PAM using RSA authorization. Users will enter the pin on the RSA application which is already provided to them during the registration. On successful pin an RSA token will be generated, which will be used to login to PAM. PAM users need to enter the pin on the application every time to generate RSA token.

10.5. Session Recording

Video recording of each session will be stored and is available for audit purpose. Video would be available on PAM for 2 years.

10.6 Approval Flow

Approval from device owner (Unit Head/Section Manager) be required in case a user needs to use L3 level account. The user can create an access request in PAM for access to L3 level privilege account for a scheduled task on scheduled date and time. If the period for which access is required exceeds the scheduled time, the user can continue the task until session is over.

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

10.7 System access procedure

All server integrated with PAM should only be accessed via PAM server. Direct access is not possible once the system is onboarded to PAM. Password will be rotated and the user will not have visibility of the current password. System owner would be responsible for that.

10.8 Emergency cases

In emergency cases, users don't have direct network access to the end devices, and they don't know the password. For network access:

Few VPN accounts with direct access to end devices can be created via IDM by respective device owners. The naming convention should be company name_crisis. Password custodian for these VPN account are device owner.

User can request password of level_4 with JIRA process [SAR]. Password must be reset after use. There are three types of break glass scenario.

10.8.1 PAM is not accessible

If primary and secondary PAM server is inaccessible, then DR will serve PAM requests. Despite high availability configured in PAM, if its inaccessible then L4 account configured in each device will be used only for emergency cases for OS as well as DB. The department head will be custodian of the credentials for the devices under their domain. Despite of HA and DR, If PAM is down, then no one would be able to login to servers as password is rotated. In Such situation, ESPP 's priority would be making PAM UP. In the meantime, if anyone needs emergency access to servers, PAM administrator/CIO would provide password to the responsible person. Once PAM is up, the password shared must be changed.

10.8.2 PAM is up but the end device is not accessible

In this case, PAM is running but some device might not be accessible via PAM hence direct login might be required to troubleshoot or recover the device. PAM Administrator can provide password via PAM upon approval from the device owner. Once device is working fine, Password must be changed

10.8.3 Device owner not available for L3 account approval

In this case, PAM admin and CIO/CTO or PAM administrator will also be able to approve L3 account request.

10.9 Password rotation


Password rotation would be as per the organization's Password Management Guidelines.

10.10 Account discovery

PAM can discover all privileged accounts once root/administrative account password is vault into PAM. The list provided by system owners of the server should match with the list of privileged accounts discovered via PAM. Else, system owner should justify the issue.

10.11 Roles Responsibility matrix

Unit/Team	Role in PAM	Description
CIO	Password Custodian	Password Custodian for devices under IT

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

CTO	Password Custodian	Password Custodian for devices under Technology
IT Services	Global Administrator	Perform all admin activates in PAM
Information Security Unit Head	Auditor	Verify log from PAM/Enforce, review and control PAM
OS, Database and planning Management Team, ESPP Unit	No role in PAM	System owner who create user and necessary role as per the guideline in the end devices
System owner		Verify admin log activities on end devices
Section Manager	Device owner	Approve/reject the L3 level access request as per business need
Unit Head	Device owner	Approve/reject the L3 level access request as per business need
End user	Normal user	Log in to end device using PAM

11 Exceptions

Any exception to the above-mentioned guideline will be handled via the exception process

12 References


- Ncell password guideline
- Information Security Policy
- Ncell Technology Policy
- Information, IT and Network Security
- Access Management Process

Annexure – I

Check list for PAM integration

System Admin / owner

- ☐ Update the System inventory detail in Asset Management [If missing]
- ☐ Approval from Security Team to add system on PAM [If not CJ]
- ☐ Open network access from PAM to your system. Source IP [10.18.12.74, 10.18.12.80, 10.19.12.74]
- ☐ Create level_1, level_2, level_3, level_4 users
- ☐ Validate permission of level_1 [Read only Access]
- ☐ Validate permission of Level_2 [Daily operation account]
- ☐ Validate permission of level_3 [Can switch to root w/o password]
- ☐ Validate level_4 account and its permission.
- ☐ Direct root login is disable
- ☐ Disable direct network access in server. Develop use case with GSOC to monitor direct access
- ☐ Prepare Crisis VPN account for break glass scenario.
- ☐ Remove all human account. Strictly use level_1, level_2, level_3 account via PAM only.
- ☐ For using service account, need to take approval of level_3 and switch to root and service account.
- ☐ Open network access request as per below information:

	Ncell	Classification: Internal
	Privileged Access Management Procedure	Owner: CIO/Head of IT
		Effective Date: 1 st October, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Windows: 3389/8550/27077/135/139/443/445-TCP

Linux: ICMP, TCP/8550, TCP/9099, TCP/9499, TCP/http, TCP/https, TCP/SSH

- ☐ Prepare or Update Access Matrix of PAM in Jira.
- ☐ Review Access Matrix of PAM on quarterly basis.

PAM Admin

- ☐ Prepare policy in PAM as per access matrix table.
- ☐ Publish role name in IDM so that user can request access from IDM.
- ☐ Schedule Level_1, level_2, level_3, root password rotation
- ☐ Set approval flow for level_3.
- ☐ Set Black list command filtering.
- ☐ Set Session recording.
- ☐ Send syslog to GSOC.

Password Custodian

- ☐ Rotate password of level_4 as per policy.
- ☐ Validate level_4 account and its permission.

Security Team

- ☐ Develop use case to monitor direct login.
- ☐ Develop use case to monitor Blacklist command.
- ☐ Develop use case to monitor Crisis VPN Login.

Crisis Scenario

- ☐ You can request level_4 password with Custodian with Jira Process. [SAR]
- ☐ You can activate crisis VPN account.
- ☐ After crisis is over, rotate the password of level_4