

Password Management Guidelines

Ncell

Guidelines

Approved Date:- 05/12/2016

Ncell	Ncell	Classification: Internal
	Password Management Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Guideline Name DOCID: GD-IT-IS-01

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
	Password Management Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Document Control

i. Document Identification

Document Title and Version:	GD-IT-IS-01 Password Management Guidelines
Effective Date:	05-12-2016
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

CEO

CIO/Head Of IT

Ncell	Ncell	Classification: Internal
	Password Management Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


v. Revision History

Rev	Date	Author	Description	Approved By	Initiated Date
0	05-12-2016	Information Security Team	Initial document	Simon Perkins	05-12-2016
1	15-08-2019	Information Security Team	Revised – Formatted, Aligned to existing processes	Vishal Mani Upadhyay	15-08-2019
2	13-12-2019	Tarani Prasad Chaudhary	Revised - Formatting	Andy Chong	13-12-2019
3	21-09-2021	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	14-12-2021
4	14-12-2021	Tarani Prasad Chaudhary	Revised - Formatting	Andy Chong	15-12-2019
5	17-Aug-2023	Information Security Team	2. Review and update: changed from annually to once in every two years 5.1.x Inactive users to be removed every 90 days 5.2.ii Password policy require all 4 type of characters Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
6	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
7	25-04-2024	Information Security Team	Re-branding 5.1.iv d. and e. added for application accounts	CIO/Head of IT	

Ncell	Ncell	Classification: Internal
	Password Management Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Table of Contents

Document Control	2
1. Purpose	5
2. Review and Updating	5
3. Scope	5
4. Roles and Responsibilities	5
4.1 System Owners	5
4.2 Information Security Officer	5
4.3 Employees	5
5. Password Management Guidelines	5
5.1 Requirements of password management systems	5
5.2 Strong Password Creation	6
5.3 Requirements for individuals responsible for provisioning user accounts	6
5.4 Requirement for individuals responsible for design and administration of systems, applications and software	6
5.5 Password Reset	7
5.6 Super User Password	7
5.7 Disabling Default Passwords	7
5.8 Recommendations for Users	7
6. Governance and Compliance	7
7. Associated Documents	8

	Ncell	Classification: Internal
	Password Management Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

1. Purpose

This document is designed to protect Ncell equipment and the information contained within those equipment by providing guidelines on handling the password as well as setting requirements for strong passwords.

2. Review and Updating

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

3. Scope

These guidelines apply to Ncell employees as well as external parties who have access to Ncell assets including but not limited to domain accounts, email accounts and accounts created and managed for and created in Ncell owned equipment.

4. Roles and Responsibilities

4.1 System Owners

System/Solution Owners shall be responsible to ensure this policy is enforced in the systems/solutions under their ownership whether by automatic or manual mechanisms.

4.2 Information Security Officer

Information Security Officer is responsible for reviewing and evaluating the need of exception raised to these guidelines if required. ISO needs to ensure that password guidelines are reviewed regularly as per the organization need.

4.3 Employees

Employees shall be responsible for following the password guidelines. They shall be responsible for keep their password safe and confidential.

5. Password Management Guidelines

5.1 Requirements of password management systems

The password management system at Ncell shall ensure the following, unless there is a system limitation:

- i. Enforcement of unique User ID and Passwords: System shall only allow individual with valid user login credentials and blank passwords shall be prohibited.
- ii. Interactive use: System shall allow users to select and change their own passwords and include a confirmation procedure to allow for input / processing errors.
- iii. Enforcement of strong passwords: Systems shall enforce the use of strong passwords. The guideline for password creation is listed in the subsequent sections of this standard
- iv. Enforcement of password maximum age: Passwords shall be changed regularly. The period shall be based on a documented risk assessment and agreed with Information Security team, else the following default shall be followed:
 - a. For user level password (e.g.: domain password) – 60 days
 - b. For application/OS/database level password of non-privileged user accounts (e.g.: CRM password, database) – 60 days
 - c. For administrative and privileged passwords – 30 days
 - d. For AD integrated application account – 90 days
 - e. For application accounts not integrated with AD – password should be manually changed, at least once a year, or else, compensating controls shall be put in place to ensure that the application accounts cannot be misused by malicious actors.
- v. Enforcement of password minimum age: System shall enforce password minimum age of 1 day.
Disclaimer: This parameter is not applicable in the Oracle Database due to system's limitations.
- vi. Enforcement of invalid logon attempts: Account shall be locked out after more than five (5) invalid logon attempts.

Ncell	Ncell	Classification: Internal
	Password Management Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- vii. Enforcement of user logout: Once a user account is locked out, it shall remain locked out for 30 minutes.
- viii. Enforcement of an error message: In case a user enters a wrong user id or password, the error message displayed by the system shall not indicate which part of the data is correct or incorrect.
- ix. Enforcement of idle time out: System/Session idle time out should be 15 minutes.
- x. Enforcement of removal of inactive users: Inactive users shall be removed every 90 days
- xi. Force users to change temporary passwords at the first login: System shall force users to change password at first login
- xii. Enforcement of password history: We shall prevent re-use of last twenty [20] passwords.
- xiii. Storage: Passwords shall be stored securely.
- xiv. Any scripts, schedule jobs or access to system tasks should not use the plain text. Password must be encrypted in that case.
- xv. Transmission systems shall ensure secure transmission of passwords by utilizing alternatives include encrypted tunnel (e.g. IPSec, SSH or SSL), using a one-way hash or implementing a ticket-based authentication.
- xvi. At least 50% of the characters shall be changed when new passwords are created in systems that support configuration of this parameter.
- xvii. Passwords shall not contain any of the following wherever applicable and supported by the systems:
 - a. Dictionary words (e.g., computer, work) or common names
 - b. Portions of associated account names (e.g., user ID, login name). Consecutive character strings (e.g., abcdef, 12345)
 - c. Simple keyboard patterns (e.g., QWERTY, asdfgh).
 - d. Generic passwords (i.e., password consisting of a variation of the word "password" [e.g., P@ssw0rd1]).
 - e. Identical characters next to each other (e.g., shddeskh)
 - f. Name of the company or brand names of products

5.2 Strong Password Creation

- i. The password shall be at least
 - a. 10 non-blank characters in length for non-privileged user accounts.
 - b. 15 non-blank characters in length for privileged user accounts.
- ii. The password complexity shall have a minimum of one character of the following requirements where applicable and supported by the systems:
 - a. English uppercase characters (E.g., A-Z)
 - b. English lowercase letters (E.g., a-z)
 - c. Non-Alphanumeric special characters (E.g., ! @, #, \$, %, ^, &, etc.)
 - d. Base 10 Digits/Numerals (E.g., 0-9)
- iii. Last twenty passwords shall not be used again.

5.3 Requirements for individuals responsible for provisioning user accounts

- i. Enforce strong passwords: Ensure only strong passwords are selected at the time of provisioning process / resetting existing user(s) password(s).
- ii. Do not select 'User cannot change the passwords': Administrator shall restrict to use this choice, at the time of provision process and/or modification process.
- iii. Do not select "Password never expires": Administrator shall restrict to use this choice, at the time of provisioning process and/or modification process.
- iv. Require a change of initial or "first-time" passwords: Users shall be forced to change the password on their first login.
- v. Never ask for a user's password: Support personnel shall not ask for user passwords for repair and/or troubleshooting purpose.

5.4 Requirement for individuals responsible for design and administration of systems, applications and software

- i. Change default account passwords: The default / built-in passwords shall be changed immediately upon installation and configuration of the system or application. Ownership of such passwords shall be documented by Information Systems Engineer.

Ncell	Ncell	Classification: Internal
	Password Management Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- ii. Storage & delegation of privileged passwords: Privileged passwords shall be kept securely (e.g. sealed envelope in a fire proof cabinet, password vault etc.) and access shall be restricted to designated individual.
- iii. Implement strict controls for system-level and shared service account passwords: All system-level passwords (e.g., root, Domain admin, NT admin, Databases, application administration accounts, etc.) must be changed on periodic basis.
- iv. Do not use the same password for different administrator accounts: Administrators shall restrict the use of same password for different administrator accounts.
- v. Do not allow passwords to be transmitted in plain-text: Passwords shall be transmitted over secure network such as IPSec, SSH or SSL connections or by implementing a ticket-based authentication scheme.
- vi. Do not store passwords in easily reversible form: Passwords shall not be stored or transmitted using weak encryption or hashing algorithms.

5.5 Password Reset

User will request for reset of password to the IT service/system owners. These teams will verify the identity of the user by verifying the employee number and then reset the password. The new password will be a one-time password and will be changed immediately when reset by the system administrator.

5.6 Super User Password

- i. All privileged user passwords for Operating Systems, Databases, Applications, Network Equipment like routers, switches etc., shall be stored securely.
- ii. All privileged user passwords will be changed once in 30 days.

5.7 Disabling Default Passwords


Vendor Supplied User-IDs/Passwords, encryption keys, and other access codes included with vendor-supplied systems will be changed before a new system goes into production. Similarly, default passwords shipped with software will be disabled or changed before the software is deployed in the production environment.

5.8 Recommendations for Users

- i. Login credentials / passwords of Ncell systems shall be maintained securely and not shared with anyone, for any purpose.
- ii. Passwords should be changed at least every 60 days and the previous 20 passwords should not be used, with the exception of service level accounts/local accounts.
- iii. Your password shall not be written /displayed at your work place or together with equipment where your password is used.
- iv. If a password has become known or is suspected to be known by other personnel, internal or external, it shall be considered as comprised and must be changed immediately.
- v. If you suspect that a password has been misused, this shall be reported immediately as a security incident at infosec@ncell.com.np or to the Information Security team members or by logging an incident at NOC.
- vi. To avoid exposure of a password in external environments, the password used to access Ncell infrastructure shall not be used in private contexts.
 - a. Dates of birth, names of family members, and other combinations of such personal details which can be connected to the individual or can be easily guessed shall not be used.

6. 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. These password guidelines shall supersede all password related Ncell policies and procedures owned/operated by concerned divisions and departments.

	Ncell	Classification: Internal
	Password Management Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

7. Associated Documents

- i. Information Security Policy
- ii. Access Management Procedure