ID & Password Management Policy

Cogent E Services Private Limited

Corporate Information Security Guidelines

COGENT E SERVICES PRIVATE LTD.
C 100, Sector 63,
Noida GautamBudh Nagar
Uttar Pradesh 201301, INDIA
.

www.cogenteservices.com

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

SECTION-I DOCUMENT DETAILS 5

DOCUMENT INFORMATION 5

DISTRIBUTION AND CONTROL 7

SECTION-II ISMS PROCEDURE FOR DOCUMENTED INFORMATION

DEFINITIONS .....

DOCUMENT MANAGEMENT .....

Objectives of Document Management .....

Components of Document Templates .....

POLICY .....

Cogent E Services INFORMATION SECURITY MANAGEMENT SYSTEM DOCUMENTATION

Manual .....

Business Processes and Procedures .....

Work Instruction's .....

Records .....

DOCUMENT NAMING CONVENTION .....

DOCUMENT NUMBERING POLICY .....

DOCUMENT VERSIONING PROCEDURE .....

Version Number Structure .....

Releasing A Document .....

Version Number Location .....

Document Properties .....

Version History .....

SECTION 3 – STAKEHOLDER - ROLES AND RESPONSIBILITIES

Stakeholder .....

Cogent E Services Matrix .....

SECTION 4 – PERFORMANCE MEASURES .....

Critical Success Factors: .....

SECTION 5 – POLICY GOVERNANCE .....

Auditing .....

Policy Clarification .....

Policy Violations .....

Compliance .....

Exceptions .....

Review .....

Reporting .....

Distribution of Policy .....

SECTION 6 – DEFINTIONS .....

SECTION 7 – APPENDIX .....

Classification of Information .....

Labeling of information .....

SECTION-I DOCUMENT DETAILS

DOCUMENT INFORMATION

Organization	**Cogent E Services Private Limited**
Document Title	ID Management System
Document Owner	Cogent E Services Chief Information Security Officer
Approved By	Information Security Steering Committee
Date Approved	07th Jun'21
Last Reviewed on	07 Jul'21
Date Published	07 Jul'21
Effective Date	11th Jul'21
Version	V 3.1
Security Classification	Internal

Preface

The Cogent E Services Information Security Management System (ISMS) Team assumes responsibility for this document and updates it as required to meet the needs of users. The Cogent E Services ISMS Team welcomes and solicits feedback from users of this document and its reference artifacts so that future revisions of this document will reflect improvements, based on new technology, organizational best practices, and lessons learned.

Copyright

VERSION CONTROL PROCEDURE

Draft Version: Any version of this document before it is finalized by all stakeholders i.e., process owners, client and ISO internal auditors, would be treated as 'Draft Version'.
The control number for the draft version would always start from '0'. For example first draft will have the control number as 0.1.

Final Version: Once the document is finalized by all stakeholders i.e., process owners, client and ISO Internal Auditor, it will cease to be a 'draft' and will be treated as 'final version'.

To distinguish between draft version and final version, the control number for finalized document would always start from an integer, greater than zero. For example, first final version will have the control number as 1.0.

Document Creation and Maintenance: This document would generally be written for the first time at the time of transition to ISO/IEC 27001:2013. It will be maintained by the Information Security Manager (ISM) and is subjected to review at a minimum on a yearly basis. The Information Security Steering Committee (ISF) members are responsible for approving any necessary amendments to the Cogent E Services Information Security Policy Documents. Changes to the Cogent E Services, ISMS Policy and ISMS Objectives shall be reviewed by the CISO and approved by Cogent E Services Information Security Steering Committee

Implementation Date: Implementation date is the date when the document is released and made operational in the ISMS. By logic, it should be after the approval date. All dates should be updated in MM/DD/YYYY format.

Amendment Procedure: The Cogent E Services Information Security Policy Documents shall be amended to reflect any changes to Cogent E Services capability or the Information Security Management System.

Summary of Changes: Version history table below denotes the nature and context of any update or change made in this document.

VERSION HISTORY

Version	Prepared by		Reviewed by		Approved by		Implementation Date	Summary of Changes
	By	Date	By	Date	By	Date		
0.1	ISM	03rd Dec'14	CISO	05th Dec'14	ISSC	--------	---------	Initial Draft
1	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	First Revision
1.0	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	New Template and updated document
1.1	ISM	13th Nov'15	CISO	13th Nov'15	ISSC	13th Nov'15	2nd Jan'16	
1.2	ISM	15th Oct'16	CISO	15th Oct'16	ISSC	15th Oct'16	31st Dec'16	
2.0	ISM	15th dec'17	CISO	15th dec'17	ISSC	15th dec'17	1st Jan'18	
2.1	ISM	22nd dec'18	CISO	22nd dec'18	ISSC	22nd dec'18	3rd Jan'19	
3.0	ISM	07th Dec'19	CISO	07th Dec'19	ISSC	07th Dec'19	10th Dec'19	
3.1	ISM	07 Jul'21	CISO	07 Jul'21	ISSC	07 Jul'21	11th Jul'21	

DISTRIBUTION AND CONTROL

Document Distribution

The Cogent E Services Chief Information Security Officer (CISO) shall distribute this document to all document change reviewer when it is first created and as changes or updates are made. The CISO shall distribute the document to members of Information Security Steering Committee (hereinafter referred to as ISSC) and Information Security Working Group (hereinafter referred to as ISWG).

The softcopy of the manual and related documents will be accessible to all employees in read-only mode through intranet server at location xxxxx

One set of hard copies will be available with the CISO as controlled copy. All other soft and hard copies of the ISMS documents are deemed to be uncontrolled. The CISO will ensure that any update to the ISMS is incorporated on the intranet server and is communicated to all employees of Cogent E Services through an appropriate mode such as e-mail.

Distribution List

Name	Title
Information Security Steering Committee	**ISSC**
Information Security Working Group	**ISWG**
Chief Information Security Officer	**CISO**

Purpose

The purpose of this plan is to ensure that all the employees involved in production have their individual IDs for processing. This also ensures information security at the work area.

Scope

All third-party Vendors are in Scope of this Doc. All ID creation and deletion should be received after due approval of the respective department owners with communication to HR.

ID Creation

1. Any APPLICATION ID Creation request for new joinee coming through NHIP program should come through training department within 5 days of batch start date
2. For any other new joinee, existing employee apart from NHIP program, ID creation request to be raised by his/her immediate supervisor after due approvals from Ops Head
3. ID creation request is sent to ID Management team with relevant details which in turn raises the request in the portal provided by Process
4. After receiving the necessary approvals from the Process Business manager, the ID creation request is processed
5. The TAT for ID creation as provided by Process is within 3 days

ID Revoke/Deletion

1. In case any employee is separated from the organization on following grounds:
    - Termination (ZTP, Code of conduct, information security breach, any other integrity issues)

- Abscond (Employee do not report to office for 3 or more consecutive days without informing his/ her immediate supervisor or any HR personnel)
- Resignation (Employee separates from the organization after serving notice period and completing all exit formalities)
- Decertified (employee not able to clear Process NHIP certification)

2. The MIS and ID management team will receive the attendance data as submitted by respective department (Ops/HR).
3. Employee status mentioned as per aforesaid terminology in the attendance record is picked up by the ID management team on weekly basis to segregate the data.

4. The ID Deletion request is processed by the ID Management team within the below mentioned time frames:
   - Terminated Employee – Same Day of termination date
   - Abscond Employee – Same Day of abscond date
   - Resigned Employee – Same Day of resigned date
   - Decertified Employee – Same Day of decertification date
   - Transferred Employee – Same Day of transfer date

ID Reconciliation

1. Local HR and ID management team do the Application ID/other ID reconciliation activity on set frequency i.e. monthly
2. Any termination/abscond/IR/Resignation/decertified case is sent for ID deletion by ID management team
3. This is tracked on daily basis by ID management team through attendance review
4. In case of IR/resigned employee, the confirmation is asked from HR team within 2 days from separation. ID deletion is processed within 3 days from resignation date
5. In case of decertified agent, the confirmation is asked from training team within 24 hrs and ID deletion is processed within 2 days from decertification date
6. In case of any issue highlighted, the same would be reported to center head for further auctioning
7. After proper RCA the issue faced is rectified and fixed

Password Management

Control Statement: Allocation of passwords for systems that are used to provide services to Client shall be controlled through a formal Password Management Process.

Explanatory Notes: Passwords shall be distributed to the users in a secure manner. The following controls relating to password management should be implemented

a. Users should be forced to change their password during the first log-on and after 30 days of each password change. However, users shall receive password change warning 15 days prior to its expiry;
b. Passwords should have combination of alpha-numeric characters and a minimum length of eight characters;
c. Passwords should have a minimum age of one day;
d. Passwords for all user and privilege accounts should expire after 30 days from its last change, with the exception of accounts used by services; password for privilege accounts should have lesser period to change the password
e. A record of five previous passwords should be maintained to prevent the re-use of these passwords
f. A maximum of three successive login failures should result in account lockout;
g. A 'locked out' user should not be able to login until the account is unlocked by the system administrator or by the user himself, using the 'Password Reset' solution
h. Passwords should not be displayed in clear text when it is being keyed in or otherwise
i. Support procedures should be in place to deal with forgotten passwords and account lockouts
j. User password resets should be performed only when requested by the individual to whom the user ID is assigned, after verification of their identity by a defined procedure
k. When passwords are reset, users should be forced to change their password to a password of their choice on the first use after the reset
l. Default accounts should be disabled and/or the associated default passwords shall be changed immediately
m. A secure 'Password List' should be maintained for all critical accounts. Only authorized individuals should have access to this 'Password List'
n. Passwords should not be coded into logon scripts, batch programs or any other executable files when user authentication or authorization is required to complete a function

Password Use

Control Statement: The Third-party shall ensure that their employees follow good security practices for the selection and use of passwords for systems that are used to provide services to Client.

Explanatory Notes: The Third-party shall ensure that users with access to information or information systems that are used to provide services to Client shall be advised for the following:

a. Keeping the passwords confidential and avoiding the recording of passwords, unless this can be stored securely and the method of storing approved;
b. Changing passwords whenever there is any indication of possible system or password compromise
c. Choosing quality password which is easy to remember but difficult to guess
d. Changing passwords at regular intervals or based on the number of accesses (passwords for privileged accounts shall be changed more frequently than normal passwords).