ISMS POLICY FOR ACCESS CONTROL

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

DOCUMENT INFORMATION

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	
3.2	ISM	07 Apr'22	CISO	07 Apr'22	ISSC	07 Apr'22	11th Apr'22	

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**

Conventions

The statements containing the words 'shall' and 'required to' in the document are mandatory rules. Failure to observe these rules may be construed as non-compliance to the policy.

The statements containing the words 'should' and 'recommended' imply a desirable requirement. Failure to adhere to these rules may not be a direct non-compliance.

SECTION-II ISMS POLICY FOR ACCESS CONTROL

BACKGROUND

INTENT

The Cogent E Services Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish an access control capability throughout Cogent E Services and its business units to help the organization implement security best practices with regard to logical security, account management, and remote access

The ISO/IEC 27001:2013 Standard **clause A.9.1.1 for Access Control r**equires that when, Cogent E Services shall: "An access control policy shall be established, documented and reviewed based on business and information securit y requirements."
The goal of access control is to allow access by authorized individuals and devices and to disallow access to all others.
On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorization and clearance may intentionally or accidentally gain unauthorized access to business information which may adversely affect day to day business.

PURPOSE

This policy establishes the Enterprise Access Control Policy, for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access through the establishment of an Access Control program. The access control program helps Cogent E Services implement security best practices with regard to logical security, account management, and remote access.
Non-compliance with this policy could have a significant effect on the efficient operation of Cogent E Services and may result in financial loss and an inability to provide necessary services to our customers. and may result in information security breaches reputation and or financial loss and an inability to provide necessary services to our customers.

SCOPE

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by Cogent E Services Any information, not specifically identified as the property of other parties, that is transmitted or stored on Cogent E Services IT resources (including e-mail, messages and files) is the property of Cogent E Services

All users (Cogent E Services employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.This policy applies at all times and should be adhered to whenever accessing Cogent E Services information in any format, and on any device.

RESPONSIBILITY

(i) Chief Information Security Officer /CISO
(ii) CPAR Owner
(iii) Project Leader/ Process owner
(iv) Team Member

EXCLUSIONS

No waivers from this Policy will be accepted.

RECORDS

1. Access Control Review
2. Access Control Matrix
3.

REFERENCE

PROCEDURE

Policy Statement

"Cogent E Services will establish specific requirements for protecting information and information systems against unauthorized access.
Cogent E Services will effectively communicate the need for information and information system access control"

ACCESS CONTROL POLICY

Business requirement for access control

The objective of this category is to control access to Cogent E Services information, information processing facilities, and business processes.

Cogent E Services **Access control policy** is based on its business needs and external requirements are established, documented and periodically reviewed. Cogent E Services Access control policy and associated controls shall take account of:

- security issues for particular data systems, given business needs, anticipated threats and vulnerabilities;
- security issues for particular types of data, given business needs, anticipated threats and vulnerabilities;
- all relevant legislative, regulatory and certificatory requirements;
- relevant contractual obligations or service level agreements;
- other organizational policies for information access, use and disclosure; and
- consistency among such policies across the organization's systems and networks;

Access control policy

The Cogent E Services Access control policy defines:

- Access control rules and rights for each user or group of users shall be clearly stated in Cogent E Services access control procedures.
- clearly stated rules and rights based on user profiles;
- consistent management of access rights across a distributed/networked environment;
- an appropriate mix of logical (technical) and physical access controls;
- segregation of access control roles -- e.g., access request, access authorization, access administration;
- requirements for formal authorization of access requests ("provisioning"); and
- Requirements for authorization and timely removal of access rights ("de-provisioning").

Access controls are both logical and physical and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The Cogent E Services Access control policy takes account of the following:

- security requirements of individual business applications;
- identification of all information related to the business applications and the risks the information is facing;
- policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information

- consistency between the access control and information classification policies of different systems and networks;
- relevant legislation and any contractual obligations regarding protection of access to data or services ;
- standard user access profiles for common job roles in the organization;
- management of access rights in a distributed and networked environment which recognizes all types of connections available;
- segregation of access control roles, e.g. access request, access authorization, access administration;
- requirements for formal authorization of access requests);
- requirements for periodic review of access controls ;
- removal of access rights

Cogent E Services has chosen to adopt the Access Control principles established in NIST SP 800-53 "Access Control," Control Family guidelines, as the official policy for this domain. The following subsections outline the Access Control standards that constitute Cogent E Services policy. Each Cogent E Services Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- **AC-1 Access Control Procedures**: All Cogent E Services Business Systems must develop, adopt or adhere to a formal, documented access control procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- **AC-2 Account Management**: All Cogent E Services Business Systems must:
  - Identify account types (i.e., individual, group, system, application, guest/anonymous, and temporary).
  - Establish conditions for group membership.
  - Identify authorized users of the information asset and specifying access privileges.
  - Require appropriate approvals for requests to establish accounts.
  - Establish, activate, modify, disable, and remove accounts.
  - Specifically authorize and monitor the use of guest/anonymous and temporary accounts.
  - Notify account managers when temporary accounts are no longer required and when information asset users are terminated, transferred, or information assets usage or need-to-know/need-to-share changes.
  - Deactivate temporary accounts that are no longer required and accounts of terminated or transferred users.
  - Grant access to the system based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by the organization or associated missions/business functions.
  - Review accounts on a **periodic basis or at least annually.**

- **AC-3 Access Enforcement**: All Cogent E Services Business Systems must enforce approved authorizations for logical access to the system in accordance with applicable policy.
- **AC-4 Information Flow Enforcement**: All Cogent E Services Business Systems must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
- **AC-5 Separation of Duties**: All Cogent E Services Business Systems must:
    - Separates duties of individuals as necessary, to prevent malevolent activity without collusion.
    - Document separation of duties.
    - Implements separation of duties through assigned information asset access authorizations.
- **AC-6 Least Privilege**: All Cogent E Services Business Systems must employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- **AC-7 System Use Notification**: All Cogent E Services Business Systems must:
    - Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with regulations, standards, and policies.
    - Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information asset.
- **AC-9 Concurrent Session Control**: All Cogent E Services Business Systems must limit the number of concurrent sessions for each system account to **ten** for information assets.
- **AC-10 Session Lock**: All Cogent E Services Business Systems must prevent further access to the information asset by initiating a session lock after **120 minutes** of inactivity or upon receiving a request from a user. In addition, Cogent E Services Business Systems must retain the session lock until the user reestablishes access using established identification and authentication procedures.
- **AC-11 Permitted Actions without Identification or Authentication**: All Cogent E Services Business Systems must identify specific user actions that can be performed on the information asset without identification or authentication. In addition, Cogent E Services Business Systems must document and provide supporting rationale in the security plan for the information asset, user actions not requiring identification and authentication.
- **AC-12 Remote Access**: All Cogent E Services Business Systems must:
    - Document allowed methods of remote access to the information assets.
    - Establish usage restrictions and implementation guidance for each allowed remote access method.
    - Monitor for unauthorized remote access to the information asset.
    - Authorize remote access to the information asset prior to connection.

- Enforce requirements for remote connections to the information asset.

- **AC-13 Wireless Access:** All Cogent E Services Business Systems must:
  - Establish usage restrictions and implementation guidance wireless access.
  - Monitor for unauthorized wireless access to the information asset.
  - Authorize wireless access to the information asset prior to connection.
  - Enforce requirements for wireless connections for the information asset.
- **AC-14 Access Control for Mobile Devices**: All Cogent E Services Business Systems must:
  - Establish usage restrictions and implementation guidance for organization-controlled mobile devices.
  - Authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information assets.
  - Monitor for unauthorized connections of mobile devices to organizational information assets.
  - Enforce requirements for the connection of mobile devices to organizational information assets.
  - Disable information asset functionality that provides the capability for automatic execution of code on mobile devices without user direction.
  - Issue specially configured mobile devices to individuals traveling to locations (international locations which are considered sensitive by the Department of State) that the organization deems to be of significant risk in accordance with organizational policies and procedures.
- **AC-15 Use of External Information Systems**: All Cogent E Services Business Systems must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information assets, allowing authorized individuals to:
  - Access the information asset from the external information systems.
  - Process, store, and/or transmit organization-controlled information using the external information systems.
- **AC-16 Publicly Accessible Content:** All Cogent E Services Business Systems must:
  - Designate individuals authorized to post information onto an organizational information system that is publicly accessible.
  - Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
  - Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system.
  - Review the content on the publicly accessible organizational information system for nonpublic information.

Removes nonpublic information from the publicly accessible organizational information system, if discovered.

User access management

This category aims to ensure authorized user access, and prevent unauthorized access, to information and information systems. Includes:

- formal procedures to control the allocation of access rights;
- procedures cover all stages in the life-cycle of user access, from provisioning to de-provisioning;
- special attention to control of privileged ("super-user") access rights; and
- Appropriate technical measures for identification and authentication to ensure compliance with defined access rights.

- **User registration**

Formal user registration and de-registration procedures shall be implemented, for granting and revoking access to all information systems and services. Control includes:

- assignment of unique user-IDs to each user;
- documentation of approval from data system owner for each user's access;
- confirmation by supervisor or other personnel that each user's access is consistent with business purposes and other security policy controls (e.g., segregation of duties);
- giving each user a written statement of their access rights and responsibilities;
- requiring users to sign statements indicating they understand the conditions of access (see also "terms and conditions of employment" and "confidentiality agreements" policies);
- ensuring service providers do not grant access until all authorization procedures are completed;
- maintaining a current record of all users authorized to use a particular system or service;
- immediately changing/eliminating access rights for users who have changed roles or left the organization;
- checking for and removing redundant or apparently unused user-IDs.

- **Privilege management**

Allocation and use of access privileges shall be restricted and controlled. Control includes:

- development of privilege profiles for each system, based on intersection of user profiles and system resources;
- granting of privileges based on these standard profiles when possible;
- a formal authorization process for all privileges;
- maintaining a current record of privileges granted;

- **User password management**

  Allocation of passwords shall be controlled through a formal management process. Control includes:

  - requiring users to sign a statement indicating they will keep their individual passwords confidential and, if applicable, any group passwords solely within the group;
  - secure methods for creating and distributing temporary, initial-use passwords;
  - forcing users to change any temporary, initial-use password;
  - development of procedures to verify a user's identity prior to providing a replacement password ("password reset");
  - prohibiting "loaning" of passwords;
  - prohibiting storage of passwords on computer systems in unprotected form; and
  - prohibiting use of default vendor passwords, where applicable.

- **Review of user access rights**

  Review of user access rights • Each user's access rights shall be periodically reviewed using a formal process. Control includes:

  - review at regular intervals, and after any status change (promotion, demotion, transfer, termination);
  - more frequent review of privileged ("super user") access rights;

User responsibilities

Control objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities

This category aims to prevent unauthorized access to, and compromise or theft of, information and information systems. It includes user awareness of:

- responsibilities for maintaining authentication security, particularly regarding password and token safety
- responsibilities for securing computers and other office equipment.

- **Password use**

  Users shall follow good security practices in the selection and use of passwords. Control includes advising/requiring users to:

  - keep passwords confidential and not "share" them;
  - avoid keeping a paper or electronic record of passwords, unless this can be done securely;

- change a password when there is any suspicion that it has been compromised, and report the suspicion;
- select "strong" passwords that are resistant to dictionary, brute force or other standard attacks;
- change passwords periodically;
- change a temporary password on first log-on;
- avoid storing passwords in automated log-on processes;
- not use the same password for business and non-business purposes;
- use the same password for multiple systems/services only where a reasonable level of security can be assured for each.

- **Unattended user equipment**

  Unattended user equipment • Users shall ensure that unattended computing equipment has appropriate protection. Unattended equipment controls include:

  - terminating active (logged-in) sessions before a device is left unattended, unless it can be securely "locked" (e.g., with a password-protected screensaver);
  - physically securing devices, or the area in which a device is located, with a key-lock or equivalent if a device will be unattended.

- **Clear desk and clear screen policy**

  Users shall ensure that desks and other work areas are kept cleared of papers and any storage media when unattended. Computer screens shall be kept clear of sensitive information when unattended.

- **Clear equipment" policy** • Photocopiers, fax machines and other office equipment shall be kept cleared of papers and any storage media when unattended.

Network access control

Control objective: To prevent unauthorized access to network services.

Policy on use of network services

Users shall only be provided with access to the services that they have been specifically authorized to use. Control includes:

- authorization procedures for determining who is allowed to access to which networks and network services, consistent with other access rights; and
- policies on deployment of technical controls to limit network connections.

- **User authentication for external connections**

  Appropriate authentication methods shall be used to control remote access to the network.

- **Equipment identification in networks**

  Where appropriate and technically feasible, access to the network shall be limited to identified devices or locations.

- **Remote diagnostic and configuration port protection**

  Physical and logical access to diagnostic and configuration ports shall be appropriately controlled. Control includes:

  - physical security for on-site diagnostic and configuration ports;
  - technical security for remote diagnostic and configuration ports; and
  - disabling/removing ports, services and similar facilities which are not required for business functionality.

- **Segregation in networks**

  Where appropriate and technically feasible, groups of information services, users and services shall be segregated on networks. Control includes:

  - separation into logical domains, each protected by a defined security perimeter; and
  - secure gateways between/among logical domains.

- **Network connection control**

  Capabilities of users to connect to the network shall be appropriately restricted, consistent with access control policies and applications requirements. Control includes:

  - filtering by connection type (e.g., messaging, email, file transfer, interactive access, applications access).

- **Network routing control**

  Routing controls shall be implemented to ensure that computer connections and information flows do not breach the access control policy of the business applications. Control includes:

  - positive source and destination address checking; and
  - routing limitations based on the access control policy.

Operating system access control

Control objective: To prevent unauthorized access to operating systems, and the data and services thereof.

Controls shall be implemented to restrict data system access to authorized users, by requiring authentication of authorized users in accordance with the defined access control policy. Controls include:

- providing mechanisms for authentication by knowledge-, token- and/or biometric-factor methods as appropriate;
- recording successful and failed system authentication attempts;
- recording the use of special system privileges; and
- issuing alarms when access security controls are breached.

- **Secure log-on procedures**

  Access to data systems shall be controlled by secure log-on procedures. Control includes:

  - display of a general notice warning about authorized and unauthorized use;
  - no display of system or application identifiers until successful log-on;
  - no display of help messages prior to successful log-on that could aid an unauthorized user;
  - validation or rejection of log-on only on completion of all input data (e.g., both user-ID and password);
  - no display of passwords as entered (e.g., hide with symbols);
  - no transmission of passwords in clear text;
  - limits on the number of unsuccessful log-on attempts in total or for a given time period;
  - logging of successful and unsuccessful log-on attempts;
  - limits on the maximum and minimum time for a log-on attempt; and
  - on successful log-on, display date/time of last successful log-on and any unsuccessful attempts;

- **User identification and authentication**

  All data system users shall have a unique identifier ("user-ID") for their personal use only. A suitable authentication technique -- knowledge-, token- and/or biometric-based -- shall be chosen to authenticate the user. Control includes:

  - shared user-IDs are employed only in exceptional circumstances, where there is a clear justification;
  - generic user-IDs (e.g., "guest") are employed only where no individual-user audit is required and limited access privileges otherwise justify the practice;
  - strength of the identification and authentication method (e.g., use of multiple authentication factors) are suitable to the sensitivity of the information being accessed; and
  - regular user activities are not performed from privileged accounts.

- **Password management system**

  Systems for managing passwords shall ensure the quality of this authentication method. Control includes:

  - log-on methods enforce use of individual user-IDs and associated passwords;
  - set/change password methods enforce choice of strong passwords;
  - force change of temporary password on first log-on;
  - enforce password change thereafter at reasonable intervals;
  - store passwords separately from application data; and
  - store and transmit passwords in encrypted form only.

- **Use of system utilities**

  Use of system utilities that are capable of overriding other controls shall be restricted, and appropriately monitored (e.g., by special event logging processes).

- **Session time-out**

  Interactive sessions shall shut down and "lock out" the user after a defined period of inactivity. Resumption of the interactive session shall require re-authentication. Control includes:

  - time-out periods that reflect risks associated with type of user, setting of use and sensitivity of the applications and data being accessed;
  - waiver or relaxation of time-out requirement when it is incompatible with a business process, provided other steps are taken to reduce vulnerabilities (e.g., removal of sensitive data, removal of network connection capabilities).

- **Limitation of connection time**

  Limitation on connection times shall be used to provide additional security for high-risk applications or remote communications capabilities. Control includes:

  - restricting connection time (e.g., to normal office hours);
  - restricting connection locations (e.g., to IP address ranges); and
  - requiring re-authentication at timed intervals.

Application and information access control

Control Objective: To prevent unauthorized access to information held in application systems

- **Information access restriction**

  Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy

Application and information access control • This category aims to prevent unauthorized access to information held in application systems.

Information access restriction • Access to information and application system functions by users and support personnel shall be restricted in accordance with a defined access control policy that is consistent with the organizational access policy.

- **Sensitive system isolation**

Sensitive system isolation • Sensitive systems shall have a dedicated (isolated) computing environment. Control includes:

- explicit identification and documentation of sensitivity by each system/application controller; and
- explicit identification and acceptance of risks when a shared facilities and/or resources must be used.

Mobile computing and teleworking

Control Objective: To ensure information security when using mobile computing and teleworking facilities.

This category aims to ensure information security when using mobile computing and teleworking facilities.

Controls shall be implemented that are commensurate with the:

- type of user(s);
- setting(s) of mobile/teleworking use; and
- sensitivity of the applications and data being accessed from mobile/teleworking settings.

- **Mobile computing and communications**

A formal procedure shall be implemented, and appropriate security measures adopted, for mobile computing and communications activities. Controls shall apply to laptop, notebook, and palmtop computers; mobile phones and "smart" phone-PDAs; and portable storage devices and media. Controls include requirements for:

- physical protection;
- data storage minimization;
- access controls;
- cryptographic techniques;
- data backups;
- anti-virus and other protective software;

- operating system and other software updating;
- secure communication (e.g., VPN) for remote access; and
- sanitization prior to transfer or disposal.

- **Teleworking**

  A formal policy shall be implemented and appropriate security measures adopted, for "teleworking" activities in off-premises locations. Control includes:

  - physical security measures at the off-premises site;
  - appropriate access controls, given reasonably anticipated threats from other users at the site (e.g., family members);
  - cryptographic techniques for data storage at and communications to/from the site;
  - data backup processes and security measures for those backup copies;
  - security measures for wired and wireless network configurations at the site;
  - policies regarding intellectual property used or created at the site, including software licensing;
  - policies regarding organizational property used at the site (e.g., organizations' computing hardware);
  - policies regarding private property used at the site (e.g., teleworkers' computing hardware); and
  - insurance coverage or other specification of financial responsibility for equipment repair or replacement.

SECTION 3 – STAKEHOLDER - ROLES AND RESPONSIBILITIES

STAKEHOLDER

Stakeholder	Roles & Responsibility
Managing Director	▪ Providing Overall Direction and leadership to Organization ▪ Ensuring that adequate resources and provisions are in place for the continued protection of Information assets of Cogent E Services.
Director Operations	▪ Ensuring quality and security issues that may affect the Cogent E Services Business and Strategic Plans are considered. ▪ Authorize and decide on new security products to be implemented across Cogent E Services
Director Corporate Affairs	▪ Ensuring continued compliance with Cogent E Services business objectives and external requirements
Information Security Steering Committee	▪ The committee shall take overall responsibility for Quality and Information security, including ▪ Ratification of the Quality Management and Information Security Policies and Procedures suggested by the CISO. ▪ Ensure that Quality and Information Security Policies and Procedures can be implemented by ensuring the involvement of the appropriate business heads. ▪ Initiating internal and external security reviews and ensuring that action is taken to rectify any shortfalls identified.
Chief Information Security Officer	▪ CISO is responsible for effectively conducting management review meetings & provides guidance for improvements. ▪ CISO is responsible for ▪ Organizing management review meetings, ▪ Reporting on performance of ISMS and ISMS at Cogent E Services ▪ Maintaining records of Management Review meetings & ▪ Take follow up actions

Stakeholder	Roles & Responsibility
	▪ Establishes and maintains process and product audit schedule. ▪ Monitors and controls the day-to-day QA activities and schedule. ▪ Escalates unresolved non-compliance issues to the ISM Committee ▪ Identifies training required to perform the tasks which includes training of the QA Group and QA orientation for the project team members.
Information Security Manager	▪ Provide direction and support for security implementation ▪ Support the risk management process by analyzing threats to the computing environment. ▪ Analyze reports submitted and the work performed by ISO 27001 Core Team and take corrective action. ▪ Ensure that ongoing information security awareness education and training is provided to all Cogent E Services employees during security project implementation ▪ In co-ordination with Internal Audit guidelines, incorporate appropriate procedures in the routine audit checks to verify the compliance to the Cogent E Services Information Security Policy and detect incidents.
Internal Auditor/s	▪ Identify areas/processes where audits are required ▪ Prepare audit plan; ▪ Select audit team member; ▪ Prepare audit report; ▪ Report audit conclusion to Information Security Steering Committee .Performs the audit using the consolidated audit checklist. ▪ Reports the non-conformities and recommends suggestions for improvement

Stakeholder	Roles & Responsibility
Information Security Coordinator and Document Controller	▪ Ensure Documents & records are stored and maintained in a central location & in proper manner for retrieval and backup ▪ Assures all documents are properly formatted ▪ Handle records according to their classification ▪ Ensure records are maintained in a proper manner for retrieval;
Head of Department	▪ Operations Representative will be responsible for preparing and maintaining Information Security Policies & Procedures within Operations at Cogent E Services. ▪ Create security awareness within Operations at Cogent E Services ▪ Provide a report of Cogent E Services Information Security Policy violations and IT security incidents as and when they occur, else a clean statement. ▪ Oversee all information security processes and serve as the focal point for all information security issues and concerns. ▪ To bring any possible security threats to the notice of Cogent E Services.
Employee /s	▪ Adhere to Cogent E Services Policy and procedure ▪ Suggest remedial measures to non-conformities detected. ▪ Suggest document change for processes if required

RACI MATRIX

The following table identifies who within Cogent E Services is Accountable, Responsible, Informed or Consulted with regards to this documented policy. The following definitions apply:

- **Responsible –** the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	**ISMS Lead Auditor**
Accountable	Corporate Information Security Officer
Consulted	ISWG
Informed	ISSC

CISO/IS Manager in their role as Cogent E Services Chief Information Security Officer are /is responsible for effectively conducting management review Meetings & provides guidance for improvements. CISO is responsible for

- Organizing management review meetings,
- Reporting on performance of Cogent E Services ISMS
- Maintaining records of Management Review meetings &
- Take follow up actions
- Identify areas/processes where audits are required
- Designate person responsible for auditing the processes
- Ensure the effective implementation of audit procedure within their area of responsibility
- Prepare audit program
- Monitor the performance of the internal audit activities;
- Present the summary of audit findings at the Management Review Meeting;
- Maintain all internal audit records.
- Ensure that the audit of the process(s) is carried out periodically and without hindrance.
- Suggest remedial measures to non-conformities detected.
- Suggest document change for processes if required.
- Designate person responsible for as Information Security Manager/ Coordinator for CAPA in the various processes
- Ensure the effective implementation of CAPA procedure within their area of responsibility

SECTION 4 – PERFORMANCE MEASURES

CRITICAL SUCCESS FACTORS:

S. No.	Critical Success Factors
1	Top Management Support & Commitment
2	Effective & Timely Management Reviews
3	Adherence to Procedure by all concerned
4	Regular Management Reviews
5	Regular Reviews of Follow-up of Actions arising from Management Reviews & Internal Audits

SECTION 5 – POLICY GOVERNANCE

AUDITING

This policy will be audited at periodic intervals by the Cogent E Services Internal Audit team as per the Information Security Management System audit plan. Audit Findings will constitute one of the significant inputs for Management Reviews of this policy document.

POLICY CLARIFICATION

For general questions or clarification on any of the information contained in this policy, please contact Cogent E Services Chief Information Security Officer For questions about department-wide Information Security policies and procedures contact the Cogent E Services Information Security Manager.

POLICY VIOLATIONS

Violations of this policy may include, but are not limited to any act that:

- Does not comply with the requirements of this policy;
- Results in loss of Cogent E Services information;
- Exposes Cogent E Services to actual or potential loss through the compromise of quality and or Information security;
- Involves the disclosure of confidential information or the unauthorized use of Cogent E Services information and information processing facilities;
- Involves the use of the hardware, software or information for unauthorized or illicit purposes which may include violation of any law, regulation or reporting requirements of any law enforcement or government body;
- Violates any laws which may be introduced by the Government from time to time in the region in which Cogent E Services is operating or providing services ;

COMPLIANCE

Violation of this policy may result in disciplinary action which may include suspension, termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of Cogent E Services Information Resources access privileges, other disciplinary actions including civil and criminal prosecution.

EXCEPTIONS

Deviations from this procedure can be exceptions or breaches. A deviation can either be permitted, or is then referred to as an exception, or not permitted, and is then referred to as a breach. Exceptions shall not be granted, unless exceptional conditions exist.
All requests for exceptions to this policy shall be addressed through the Cogent E Services Chief Information Security Officer
Requests for exceptions to policies must have a justifiable business case documented and must have the necessary approvals. Exceptions must be approved and signed by either:

- Managing Director, Cogent E Services Pvt. Ltd.
- Chief Information Security Officer

Once approved, exceptions to policy will be valid for a pre-decided period after which it must be re-

evaluated and re-approved. All exceptions to policy must be communicated to Corporate Information Security Officer (CISO) or Information Security Manager (ISM) and captured in a Log by the Document controller.
If policy exceptions are likely to circumvent existing internal controls then “Mitigating Controls” or “Compensating Controls” must be implemented and followed. The Cogent E Services ISMS Committee must be involved in all instances where Information Security controls are bypassed.

REVIEW

This policy must be reviewed once a year at a minimum or as the need arises along with all the stakeholders involved in this procedure and be re approved by Cogent E Services Information Security Steering Committee accordingly.

REPORTING

Any person who becomes aware of any Information Security issues, risks and or loss, compromise, or possible compromise of information, or any other incident which has Information Security implications, must immediately inform his/her immediate superior authority as the case may be, who shall initiate immediate action to prevent further compromise or loss.

DISTRIBUTION OF POLICY

The Policy is an internal document and is meant for internal usage within the company. Duplication and distribution of this policy without an authorized release is prohibited. The Cogent E Services ISMS Team will decide on the number of copies that will be in circulation and the persons with whom the document will be available.

Every person in custody of the document has the responsibility for ensuring its usage limited to “within the organization”. The custodian of the document will also ensure and that the document is continually updated with amendments that may be issued from time to time. Any loss or mutilation of the document must be reported promptly to the Cogent E Services Information Security Manager.

SECTION 6 – DEFINTIONS

Word/Term	Definition
CPAR	Corrective and Preventive Action Report
Corrective action	Remedial action for rectifying work incorrectly done in the past, in order to comply with ISO requirement. Action to eliminate the cause of a detected nonconformity or other undesirable situation.
Preventive action	Action for eliminating the root cause of a problem, in order to prevent it from happening again in future. Action to eliminate the cause of a potential nonconformity or other undesirable potential situation.
Conformity	Fulfillment of a requirement.
Nonconformity/Non-conformance:	Non-fulfillment of a requirement
Root Cause	Fundamental deficiency that results in a non-conformance and must be corrected to prevent recurrence of the same or similar non conformance
Continual Improvement	recurring process which results in enhancement of Information Security performance and the Information Security management system NOTE 1 The process of establishing objectives and finding opportunities for improvement is a continual process. NOTE 2 Continual improvement achieves improvements in overall Information Security performance, consistent with the organization's Information Security policy. *Is a process or productivity improvement tool intended to have a stable and consistent growth and improvement of all the segments of a process or processes? ... (Also called incremental improvement or staircase improvement).The process of establishing objectives and finding opportunities for improvement is a continual process through the use of audit findings and audit conclusions, analysis of data, management reviews or other means and generally leads to corrective action or preventive action.*
Defect	Non-fulfillment of a requirement related to an intended or specified use.
Project/Process Owner	Person having the responsibility and authority to accomplish/implement a specific activity or process (includes organizational line managers, project managers, etc.)

SECTION 7 – APPENDIX

APPLICABLE FORMATS

CORRECTIVE ACTION REQUEST

☐ Internal

☐

(A) DETAILS TO BE COMPLETED BY ORIGINATOR

To :	From : (Originator) (Name / Signatory / Designation / Department)	
Description of Activity / Product / Process / Services / System	CAR No.:	Date :
	Reference to this CA being generated (Customer Complaint / Internal Reject)	
Description of Non-Conformity *		

(B) DETAILS TO BE COMPLETED BY RESPONSIBLE FUNCTION

Root Cause(s) *	
Action Taken to Prevent Recurrence *	
Change in Procedure (if any) *	
Time Frame for CA to be taken (by date)	Completed by Responsible Function (Name / Signatory / Designation / Department)

(C) DETAILS TO BE COMPLETED BY VERIFICATION AND FOLLOW-UP AUTHORITY

Verified close-out by Originator ☐ Accept ☐ Reject	Follow-up (if necessary) by Originator : _____

_____ (Name / Signatory / Date)	(Name / Signatory / Date)
If Rejected - Reason for Rejection *	**Further Action Required ***

Corrective Action/Preventive Action Request (CAR/PAR) Tracking Log

CAR/PAR #	*Source	Assigned to	Issue Date	Due Date	Closed (Y/N)	Reported (Y/N)

*Source:

IA = Internal Audit
SEC A = Security Assessment
ExA = External Audit
LN = Legal Noncompliance
MM = Monitoring and Measurement
MR = Management Review
ON = Noncompliance with Other Security Requirement Subscribed To
O = Other

CORRECTIVE ACTION TAKEN REPORT

Corrective Action Report										
Corrective Action or Preventive Action Request Serial No :	1	2	3	4	5	6	7	8	9	10
Non Conformance Report Serial No :										
Description of Non Conformance										
Audit Criteria Reference										
Management System Document Reference										
Root Cause Analysis										
Root Cause Assigned to										
Date Root Cause Assigned										
Correction										
Corrective Action Plan										
Preventive Action Plan										
Action Assigned to										
Proposed Implementation Date										
Follow up assigned to:										
Date of Follow up										
Date of Nonconformity Close out										
Verification of Effectiveness of CAPA										
Nonconformity Close out verified By										
Notes										

END OF DOCUMENT