CHANGE 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

Table of Contents

Contents

SECTION-I DOCUMENT DETAILS

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 artefacts so that future revisions of this document will reflect improvements, based on new technology, organizational best practices, and lessons learned.

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.

1. SECTION-II ISMS CHANGE MANAGEMENT

Changes to Cogent E Services (P) Ltd. information technology facilities and systems must be controlled in order to ensure that changes made to a production component are applied in a controlled and consistent manner

Explanatory Notes

Changes/Addition/Removal of information processing facilities and systems should be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures.

2. **Scope of Change Management Policy**
   - The change management policy apply to all changes to the following areas:
     - Changes to Operating systems, which must include application of patches and service packs, configuration changes, and version upgrades.
     - Changes to applications, which must include application of patches, configuration changes, and version upgrades.
     - Changes to networks and network devices like routers, switches, firewall, etc. This must include changes to router and switch configurations, IOS, firewall policy changes, network layout/traffic changes and changes to intrusion detection systems.
     - Changes to IT hardware such as change of RAM, CPU, and HDDs etc.
     - Additions of new location/new application/new Hardware to the existing setup
   - The Change Management policy address the following:
     - Change Management and documentation
     - Change Approval mechanism
     - Testing of Changes and backup
     - Unscheduled/Emergency backups

3. Policy Details

3.1 Change Management and Documentation

- The change management process must involve documenting and managing the change requests.
- The documentation must provide for a brief description of the changes requested, the date on which the request was made, prioritizing of the request, tracking and controlling modifications and assigning a unique number to each request.
- All changes must be scheduled and all the affected parties must be informed in advance of the change
- All changes have to be reviewed after the roll out.

3.2 Change Approval

- The immediate controlling authority of the user requesting the change must approve all change requests, based on business requirements. This request will be forwarded to the Head IT or higher which will then be forwarded post validation to the change request handling team from the IT department or ask for more clarifications from the end user.
- If the change request involves incorporating data from a different application, the Data Owner of that application must also need to approve the request.
- An assessment of the proposed system changes must be performed to assess its potential impact on Cogent E Services (P) Ltd. computing systems before its approval

3.3 Testing of Changes and Backup

- All changes must be tested before being carried out in the live/ production environment, wherever required.
- A quality assurance test of the changes to be implemented must be performed in a test environment prior to implementation in the production environment

wherever applicable.

- A backup of the system impacted by the change must be made prior to its being updated.
- For critical systems Rollback and recovery procedures in case of unsuccessful changes must be followed.

3.4 Unscheduled/Emergency Changes

- Unscheduled/emergency changes must be carried out only in case there are critical production issues, which require the change to be carried out.
- Any unscheduled changes must not be done without proper approval
- An audit trail of the emergency activity must also be generated which logs all activity, including but not limited to:
    - The user-ID making the change
    - Time and date
    - The commands executed
    - The program and data files affected
- After unscheduled changes are carried out, normal change procedures must be expedited.

3.5 User ID and Access Changes

- Any changes to user id including changes to the authorization levels must be done by following the procedure defined in Logical Access Control policy
- The change must involve raising a request and approval of the same by his/her supervisor as well as from the Head of Department (HOD) of the person requesting access.
- All changes must be documented and a trail must be maintained by means of preserving the change requests

3.6 Hardware Changes

- Any changes to hardware must be done by following the change management

process which includes raising of change request, approval by the appropriate authorities and documentation of the same

- The custodian of the hardware must conduct all the hardware changes after due approval of the change
- Changes done to the hardware must be updated in the hardware/Asset register after the change is done
- Changes done to the hardware must be monitored after the change to ensure that there is no untoward affect due to the change

3.7 Operation System and Application Changes

- Any change to the operating system or application must be strictly controlled by the use of the change management process, which will include raising of change request, testing, approval by the appropriate authorities and documentation of the same
- Following the steps mentioned in the documented operating procedures, wherever applicable, must do changes to the operating system or the application.
- All changes must be documented and a trail must be maintained by means of preserving the change requests
- Any change that involves downtime or disruption of services must be done after giving an appropriate notification to the affected users.

3.8 Patch and Service pack management

- Application of patches must be done in a controlled manner.
- Only tested and alpha versions of the patch or service pack must be considered for application, wherever needed.
- The patch or service pack must be obtained directly from the vendor or downloaded from the vendor site only.
- On successful testing by the nominated personnel defined and the functional

users, the patch must be applied on the production systems with approval from Head IT or higher.

- For desktop related patches, the application must be done in a scheduled manner using change request form.

3.9 Addition of hardware/Software and any other IT resource

All hardware or any other resource addition or removal of it from the production environment would be controlled and approved and a complete track of it maintained to ensure non-disruption to the operating environment

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

Stakeholder	Roles & Responsibility
	ISMS at Cogent E Services ▪ Maintaining records of Management Review meetings & ▪ Take follow up actions ▪ 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

Stakeholder	Roles & Responsibility
	Security Steering Committee .Performs the audit using the consolidated audit checklist. ▪ Reports the non-conformities and recommends suggestions for improvement
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
Information Security Management System (*ISMS*)	Management system to direct and control an organization with regard to Information Security.
Top Management	Person or group of people who direct and control an organization at the highest level.
Effectiveness	Extent to which planned activities are realized and planned results achieved.
Efficiency	Relationship between the results achieved and the resources used
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
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.*

SECTION 7 – APPENDIX

APPLICABLE FORMATS

END OF DOCUMENT