ISMS PROCEDURE FOR MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

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

VERSION CONTROL PROCEDURE 5

VERSION HISTORY 7

DISTRIBUTION AND CONTROL 7

SECTION-II ISMS PROCEDURE FOR MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION 8

BACKGROUND 8

PURPOSE 9

SCOPE 9

RESPONSIBILITY 9

EXCLUSIONS 10

RECORDS 10

REFERENCE 10

PROCEDURE 10

SECTION 3 – STAKEHOLDER - ROLES AND RESPONSIBILITIES 17

STAKEHOLDER 17

RACI MATRIX 20

SECTION 5 – POLICY GOVERNANCE 23

AUDITING 23

POLICY CLARIFICATION 23

POLICY VIOLATIONS 23

COMPLIANCE 23

EXCEPTIONS 23

REVIEW 24

REPORTING 24

DISTRIBUTION OF POLICY 24

SECTION 6 – DEFINTIONS 25

SECTION 7 – APPENDIX 26

APPLICABLE FORMATS 26

SECTION 3 – STAKEHOLDER - ROLES AND RESPONSIBILITIES..... 26

STAKEHOLDER 26

RACI MATRIX 29

SECTION 5 – POLICY GOVERNANCE..... 32

AUDITING 32

POLICY CLARIFICATION 32

POLICY VIOLATIONS 32

COMPLIANCE 32

EXCEPTIONS 32

REVIEW 33

REPORTING 33

DISTRIBUTION OF POLICY 33

SECTION 6 – DEFINTIONS..... 34

SECTION 7 – APPENDIX..... 35

APPLICABLE FORMATS 35

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 PROCEDURE FOR MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

BACKGROUND

The ISO/IEC 27001:2013 Standard **Clause 9.1 Monitoring, measurement, analysis and evaluation** states that "The organization he organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
c) when the monitoring and measuring shall be performed;
d) who shall monitor and measure;
e) when the results from monitoring and measurement shall be analysed and evaluated; and
f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

NOTE The methods selected should produce comparable and reproducible results to be considered valid.

PURPOSE

This procedure describes the overall requirements for monitoring and measurement as part of Cogent E Services 's ISMS requirements to ensure that there is adequate control on ISMS aspects, compliance with legal and other requirements, and to ISMS achieve objectives and targets

The purpose is to establish a consistent process for monitoring and measuring the key characteristics of the organization's activities, products, and services (e.g., processes), that contribute to significant to its Information Security Management System and for ensuring that equipment used to monitor/measure performance related to these processes is properly calibrated.

The intent of such monitoring and measuring is to track ISMS performance, assess implementation and effectiveness of operational controls, and track performance on objectives and targets.

of the Information Security Management System of Cogent E Services

SCOPE

This procedure addresses operations and activities that can have a significant impact on the Information Security Management, and applies to the Cogent E Services Information Security Management System (ISMS) Core Team members and personnel with monitoring and measurement responsibilities.. This procedure Includes monitoring, measuring and documenting:

I. The performance of Cogent E Services Information Security Management System,
II. The conformance with Operational Controls,
III. The progress towards completing the ISMS Programs and achieving the approved Objectives and Targets of Cogent E Services , as well as,
IV. The calibration of equipment monitoring critical processes of the significant ISMS aspects.
V. Regulations, Laws and Other Requirements Cogent E Services under the scope its ISMS

It applies to monitoring and measuring all Significant Information Security Management activities and Programmes established by Cogent E Services under the scope its ISMS . All the Organization's information systems are subject to this procedure

RESPONSIBILITY

i. Corporate Information Security Officer /CISO

a. Organizing Internal Audits, monitoring and measurement activities management review meetings,
b. Reporting on performance of Information Security Management System
c. Improve Information Security efficiency and Information Security saving through maintenance and behavior changes by your own employees
d. Take follow up actions for ensuring continual improvements

ii. The Information Security Manager performs the risk assessment to identify the type and level of audit logging and monitoring that might be required for each individual information asset.

iii. Owners of individual assets are responsible for identifying and agreeing with the Information Security Manager the logging and monitoring capabilities of the assets they own and for having them configured to meet the requirements of the risk assessment.

iv. The ISMS Coordinator is responsible for ensuring that the required monitoring activity takes place using, where necessary, outside contractors to confirm that configuration is in line with requirements of this procedure.

v. The Head of IT is responsible for configuring the information systems to meet the requirements of this procedure.

EXCLUSIONS No waivers from this Policy will be accepted.

RECORDS
(i) Information Security Management Plans (ISMPs)
(ii) Annual Information Security Improvement Plan(ISIPs)
(iii) Master List Of All Monitoring And Measuring Requirements
(iv) Monitoring And Measurement Report

REFERENCE ISMS Objectives and Metrics based on ISO 27001: 2013

PROCEDURE As Given below

The CISO, in consultation with the ISSC and the executive responsible for relevant projects / functions / departments if necessary, shall establish monitoring criteria in the following areas:

i. The achievement of ISMS objectives and targets and the progress of programmes.
ii. The effectiveness of operational control procedures for controlling the significant ISMS aspects of project activities including the control and monitoring of contractors' ISMS performance.
iii. The conformity of legal requirements and other requirements related to Cogent E Services ISMS .

After an objective and target is developed and approved, Information Security Management Plans (ISMPs) are created to specify the implementation details. These details are further described in the Objectives, Targets, and Management Programs Procedures.

Performance indicators (Pis) are assigned to each associated objective and target and are developed to monitor the key characteristics relative to the objective and target.

As new projects arise or existing activities change, the affected Department will

review the projects/activities to determine if new monitoring and measurement requirements are needed and adjust their performance indicators if appropriate.

The CISO compiles PI data and provides periodic updates to senior management at annual review meetings. It will include specific details on:

- What parameter to monitor and measure.
- How such measurement is to occur (including frequency).
- Record keeping.
- Reporting of measurements, including deviations from normal operations.
- Reference to appropriate calibration of equipment, as necessary.

Certain monitoring equipment is used to monitor operations that have an Information Security impact. Calibration of this equipment is managed and maintained by the affected department.

Resources

The CISO shall ensure appropriate resources (financial, human, technological) are available to monitor and measure the selected parameters.

Training

The CISO shall ensure training is provided on monitoring and measurement methods

Collection of Data

The CISO shall ensure that the Monitoring & Measurement data from the identified activities, products, and services is collected. This report could include initial data to establish baseline conditions for future comparison, and would be structured as a minimum to:

- Provide status of Information Security Management Programs designed to fulfill Information Security Objectives & Targets.
- Provide status of performance indicators as related to targeted timeframes,
- Provide compliance status of Information Security operating permits issued by Information Security regulatory agencies.

Performance Tracking

Information Security data collected to reflect Information Security performance is to be maintained in such a manner to allow the evaluation of progress toward realizing Information Security Objectives & Targets.

Regulations, Laws and Other Requirements

Ensure that compliance regulations, laws and other requirements are monitored. This will be accomplished by conducting a Compliance Audit every year

Key IT Systems Parameter/s that are to be measured and recorded are:

Audit logging

The servers/systems/devices for which user activity audit logging is configured,and the audit logging software that is deployed together with the schedule/matrix of audit log requirements and reporting regularity are set out in a table in appendix below.
System administrators are prohibited from erasing or de-activating logs of their own activities and the technical configuration of this control is ensured.
The schedule/matrix of audit log requirements and the audit log reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.

Monitoring system use

The servers/systems/devices for which user activity monitoring is configured, together with the schedule/matrix of monitoring requirements and reporting regularity are set out in table in appendix below.
System administrators are prohibited from erasing or de-activating logs of their own activities and the technical configuration of this control is ensured.
The schedule/matrix of monitoring requirements and the monitoring reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.

Monitoring reports are reviewed at define regularity and responsibility. Any evidence of system misuse is reported to the Information Security Manager who investigates further, and the disciplinary process may be invoked.

Protection of log information

Audit logging is configured as set out above.
Administrators are prohibited from disabling logging activity; disabling audit logs or tampering with audit log information is treated as a serious offence in the disciplinary policy and may result in immediate dismissal.

Administrator and operator logs

The servers/systems/devices for which administrator/operator activities are logged and the logging software that is deployed together with the schedule/matrix of administrator and operator activity log requirements and reporting regularity are set out in a table in appendix below.

System administrators are prohibited from erasing or de-activating logs of their own activities and the technical configuration of this control is ensured .
The schedule/matrix of activity log requirements and the log reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.
The following data protection or privacy protection restrictions also apply

Describe how administrator and operator logs and event types are investigated, what tools might be used, etc .

Fault logging

The Organization deals with error and fault logging as follows:
Here you should insert details about how you deal with these issues,

Clock synchronization

The clocks of all information systems within Cogent E Services or if necessary specify in a schedule different points of synchronization for geographically dispersed systems are synchronized with specify what and how the synchronization is performed across the network .

Throughout its information systems, the date stamp format used by Cogent E Services is: dd/mm/yyyy. The timestamp format used by Cogent E Services is hhmm, applying the 24-hour clock.

The clocks on all servers and all Organizational information processing devices (including laptops, PDAs) are checked on a regularity? Basishow and by whom ? and corrected where necessary. The record of completed checks and any necessary corrections is forwarded to the Head of IT .

Monitoring and measuring allows decision makers to determine whether or not a specific process is operating within specific parameters and, if not, where changes need to be made in the process to achieve the desired level of performance.

In considering what to measure/monitor relative to ISMS performance there are generally three categories of requirements that should be considered:
1) things that are monitored through taking quantitative measurements
2) things that are monitored through a single assessment, and
3) things that are monitored through examining trends (i.e., progress toward achieving objectives and targets).

To this end, the Corporate Information Security Officer (CISO), or their designee, will develop and maintain a **Master List of All Monitoring and Measuring Requirements**, particularly the examination of progress toward achieving objectives and targets.

The Master List of Monitoring and Measuring requirements is intended to be a "living document" in that it should be updated whenever new requirements are discerned throughout the ISMS cycle.

In developing the list, the Corporate Information Security Officer (CISO) should consider the various objectives, targets, tasks, and requirements specified in the various Management Programmes (MPs), as well as requirements related to the

maintenance of operational controls. In addition, the Corporate Information Security Officer (CISO) should consider any underlying activities that "feed into" the processes being monitored/measured to determine if monitoring/ measuring at these subordinate levels will enhance the ability of the organization to make better and more informed decisions regarding its performance.

At a minimum the master list of monitoring and measuring requirements shall include the:

- MP and/or OC from which the monitoring/measuring requirement is derived;
- Parameters and/or processes being monitored/measured;
- Frequency of measuring/monitoring;
- Person responsible; and
- Location of the appropriate record.

3. Periodically, but at least once each ISMS cycle, the Corporate Information Security Officer (CISO)and others, as appropriate, will review the master list of monitoring and measuring requirements to determine if it is sufficient to adequately track the performance of the ISMS and/or to make adequately informed decisions about the organization 's performance. If it is determined that additional monitoring and/or measurements are needed, the Corporate Information Security Officer (CISO) will work with the appropriate manager responsible for the process to develop the indicator and then add it to the Master List.

4. The Corporate Information Security Officer (CISO), or their designee, shall develop a master list of all equipment that requires calibration and is used to monitor/measure performance within the organization's ISMS (an ISMS document). This list shall include the name, manufacturer, model number of each piece of equipment; the frequency of calibration; when the last calibration was completed and when the next is due; who is responsible for the calibration; and the location of the calibration record.

The list of equipment requiring calibration should be reviewed and updated whenever the Master List of Monitoring and Measuring Requirements is reviewed to ensure any new equipment is identified and added to the calibration list. In addition, the Corporate Information Security Officer (CISO) should contact the person(s) responsible for ensuring equipment calibrations are completed as needed to update the list with new last and next calibration dates.

6. Monitoring criteria shall include the monitoring / measuring frequency, methods, responsibilities and records or reports that shall be kept. The monitoring criteria shall be documented or integrated into the respective operational control procedures (refer OCP's)

The responsible Project / Function / Departmental Manager shall ensure that the monitoring requirements are carried out and report any ISMS nonconformities to the Corporate Information Security Officer (CISO).

7. The ISSC shall hold regular meetings (approximately every 3 months) and maintain records to:

I. discuss and review the achievement of the objectives and targets and the progress of relevant programmes;
II. review the monitoring data (e.g. inspection checklists) to check whether the monitoring and operational control procedures are implemented properly;
III. review information to evaluate whether Cogent E Services activities comply with applicable ISMS legislation and other requirements identified ;
IV. review any ISMS nonconformities, and the corresponding corrective action and preventive action

In case of nonconformities, the relevant Project / Function / Departmental Manager shall investigate the causes of nonconformities and establish appropriate corrective and preventive actions. The corrective and preventive actions shall be verified by the Project / Function / Departmental Manager and endorsed by the CISO).

The monitoring criteria shall be reviewed and revised according to changes in legislative requirements and the practical situations of Cogent E Services 's a result of continual improvement of ISMS performance. Whenever necessary, calibration of measuring equipment shall be defined clearly in terms of calibration methodology, calibration frequency, acceptance criteria and responsible personnel.
Cogent E Services shall record the results (and maintain the records) of the periodic evaluation of compliance and shall be considered at the management review.

Process Inputs:

S. No.	Input	Source	Frequency	Reference
a.	Management Review Records	MR	3 Month	
b.	Maintenance Records	Head Maintenance	Monthly	
c.	Supplier Performance Records	Head Purchase	3 Month	
d.	Product & Process Performance Record	Head Production	3 Month	
e.	Internal Audit Records	MR	3 Month	

Process Output:

S. No.	Outputs	To	Reference
a.	Information Security Management System Improvement Project Report	Concerned Dept.	

b.	Action Plans for Information Security Management System Improvements	-do-	

Process Monitoring:

S. No.	Monitoring Brief	Responsibility	Frequency	Reference
a.	Continual Improvement Project Status	MR	3 Month	
b.	Benefit Status of Completed Project	Concerned Head	After Completion	

Benefits

- Increase return on Information Security -related investments.
- Assist you in your pursuit of ambitious goals to get results that stick. Help boost productivity and overall business performance.
- Map the Information Security management plan directly to government requirements and mandates.
- Support response to shareholder inquiries.
- Generate accurate savings metrics to support communications and public relations campaigns.

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

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

- Master List Of All Monitoring And Measuring Requirements
- Monitoring And Measurement Report

END OF DOCUMENT