INCIDENT 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

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 http://192.168.254.199/ems/ISMS

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 INCIDENT MANAGEMENT

Incident management responsibilities and procedures will be established to ensure quick, effective and orderly response to security incidents**.**

Explanatory Notes

The term 'incident' in this document can be defined as any irregular or adverse event, which occurs on any part of COGENT E SERVICES PRIVATE LIMITED's information systems. Incident management responsibilities and procedures should be clearly defined. This would help to minimize the damage from security incidents and malfunctions and help to monitor and learn from security incidents

Policy Details

1.1.1 Incident Management Coverage

- Incident management procedures must cover all types of potential security incidents, including:
  - Theft of / damage to computer hardware equipment and communication network;
  - Information system failures and loss of service;
  - Illegal access to a system;
  - Deliberate denial of service;
  - Virus and Worm incidents;
  - Errors resulting from incomplete or inaccurate business data;
  - Errors resulting from inaccurate processing of data/human error;
  - Breaches of confidentiality;
- In addition to normal contingency plans to recover from such incidents, incident management procedures must cover:
  - Analysis and identification of the cause of the incident;
  - Planning and implementation of remedies to prevent recurrence;
  - Collection of audit trails and similar evidence;
  - Communication with those affected by or involved with recovery from the incident;

1.1.2 Incident Handling Procedures

- Action to correct and recover from security breaches and system failures must be controlled. The procedures for Incidence response ensure that:
  - Clearly identified and authorized staff are allowed access to production systems and data;
  - All emergency actions taken are documented in detail;
  - Emergency action is reported to management and reviewed in an orderly manner;

- The integrity of business systems and controls is confirmed with minimal delay;

- Audit trails and similar evidence must be collected and secured, as appropriate, for:
  - Internal problem analysis;
  - Use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings e.g. under Copyrights Act, Information Technology Act;
  - Negotiating for compensation from software and service suppliers;
  - Settlement of Insurance claims, wherever applicable.

1.1.3 Reporting Software Malfunctions

- Users should report any software malfunctions, software not functioning correctly i.e. as per the specification (suspected malicious software, such as virus infection).
- Software malfunctions or errors must be reported to the system administrators or the help desk. As part of the reporting users will be required to note any symptoms, error messages, or failures.
- The respective departments must notify ISM if the software malfunction is in any way suspected or indicative of security vulnerability.
- The users, in the case of software malfunction are expected to follow the following procedures:
  - Note the symptom of problem and any messages appearing on the screen; and
  - If a security breach is suspected (e.g. suspicious mail client behavior), the user should inform the system administrator immediately for appropriate remedial action.
  - The computer should not be used until such time a clearance is obtained from the system administrators for usage of the computer.

Also, the data/diskettes will not be transferred to other computers.

- In case the system administrators suspect a security breach after the preliminary assessment of the incident, they should report the matter immediately to the ISM.
- The users should be warned not to attempt to remove malfunctioning software, without the support of IT.

1.1.4 Log Book

- A written log must be kept for all security incidents, which are under investigation.
- The information must be logged in a location and format that cannot be accessed and altered by others.
- The types of information that must be logged are:
  - Dates and times of incident and receipt of information.
  - Names of information system components (e.g. systems, programs or networks) that have been affected.
  - People contacted.
  - Emergency actions taken.

1.1.5 Release of Information

Control of information during the course of a security incident or investigation of possible incident is very important. Providing incorrect information to the wrong people can have undesirable side effects, especially if the news media is involved.

- All information during the course of a security Incident or investigations of a possible incident must be controlled.
- All release of information must be authorized by the CISC.
- All requests for press release must be forwarded to the Administrative Office Head/Corporate Communications.

1.1.6 Learning from incidents

- A follow-up analysis of the incident must be performed after an incident has

been fully handled and all systems have been restored to a normal mode of operation.

- A security incident report must be prepared by a person designated by the incident co-ordination team.

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	▪ CISO is responsible for effectively

Stakeholder	Roles & Responsibility
Security Officer	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 ▪ 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

Stakeholder	Roles & Responsibility
	▪ 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
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 event	identified occurrence of a system, service or net work state indicating a possible breach of information securit y policy or failure of controls, or a previously unknown situation that may be securit y relevant
information security incident	single or a series of unwanted or unexpected *information security events* that have a significant probabilit y of compromising business operations and threatening *information security*
information security incident management	*processes* for detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents*
information sharing community	group of organizations that agree to share information Note 1 to entry: An organization can be an individual.
information system	applications, services, information technology assets, or other information handling components
information security continuity	*processes* and procedures for ensuring continued *information security* operations
information processing facilities	any information processing system, service or infrastructure, or the physical location housing it

SECTION 7 – APPENDIX

APPLICABLE FORMATS

Security Incident Report								
Incident Reg. No.					Incident Date			
Incident Details: A								
Responsible Person		System Admin			Department		Technology	
TAT on Correction				TAT on Corrective action				
Correction								
Root Cause Analysis								
Decision of ISMS Forum						Date		
Corrective & Preventive Action Details								

Security Incident Report						
CISO Audit & Findings	**Name**				**Date**	
Information to ISMS Forum					**Date**	
Final Closure Status: Closed.						

INCIDENT REPORT TRACKER

Month:

Sr. No	Location	Incident No.	Incident Description	Severity	Downtime	Status

END OF DOCUMENT