PHYSICAL & ENVIRONMENTAL SECURITY POLICY

Cogent E Services Private Limited

Corporate Information Security Guidelines

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

www.cogenteservices.com

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

SECTION-I DOCUMENT DETAILS

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 PHYSICAL & ENVIRONMENTAL SECURITY POLICY

Objective • Unauthorized physical access, loss, damage or interference to Cogent E Services premises and infrastructure, or interruptions to its critical operations, should be prevented using physical and environmental controls appropriate to the identified risks and the value of the assets protected.

SECURE AREAS

Physical security perimeter

Physical security perimeter • In Cogent E Services Security perimeters should be used to protect sensitive areas that contain information and information processing facilities. Physical security for other Cogent E Services offices, rooms and facilities should also be designed and implemented, commensurate to the identified risks and the value of the assets at risk in each setting. This could include:

- clearly defined and marked perimeters, except in situations where hidden or disguised perimeters would enhance security;
- restrictions on information about facilities, including directory and location information, where this would enhance security;
- use of perimeter walls, windows and doors, protected with bars, locks, alarms and other supplemental measures as appropriate;
- controlled entry doors/gates, with manned reception desks or automated lock/ID systems, to control passage into the restricted area;
- use of additional physical barriers, where appropriate to prevent unauthorized access or physical contamination;

- provision of appropriate protection against fire, water or other reasonably anticipated environmental threats;
- use of appropriate intrusion detection systems, such as motion and perimeter alarms, audio and video surveillance; and
- measures designed with sufficient redundancy , such that a single point of failure does not compromise security.

Physical entry controls

Physical entry control • In Cogent E Services sensitive areas of information processing facilities should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Appropriate entry controls for other offices, rooms and facilities should also be designed and implemented, commensurate to the identified risks and the value of the assets at risk in each setting. This could include:

- password, "token" or biometric authentication mechanisms for entry points (e.g., keycard and/or PIN);
- supplementing automated authentication methods with security personnel on site, where appropriate for highly sensitive assets;
- recording of date/time of entry and exit, and/or video recording of activities in the entry/exit area, as appropriate;
- requirement for authorized personnel to wear visible identification, and to report persons without such identification;
- appropriate authorization and monitoring procedures for third-party personnel who must be given access to the restricted area; and
- regular review and, when indicated, revocation of access rights to secure areas .
- Use of highly visible controls, where appropriate as a deterrent;
- Use of unobtrusive or hidden controls/facilities, where appropriate for highly sensitive assets.

Securing offices, rooms, and facilities

Protecting against external and environmental threat

Protection against external and environmental threats • In Cogent E Services physical protection against damage from fire, flood, wind, earthquake, explosion, civil unrest and other forms of natural and man-made risk should be designed and implemented. This could include:

- consideration of probabilities of various categories of risks and value of assets to be protected against those risks;
- consideration of security threats posed by neighboring facilities and structures;
- appropriate equipment (e.g., fire-fighting devices) and other counter-measures provided and suitably located on site; and
- Appropriate off-site/remote location for backup facilities and data copies.

Working in secure areas

Working in sensitive areas • Protective measures and guidelines for working in sensitive areas should be designed and implemented. This could include:

- limiting personnel's awareness of, and activities within, a sensitive location on a need-to-know/need-to-do basis;
- limiting or prohibiting unsupervised/unmonitored work in sensitive areas, both for safety reasons and to avoid opportunities for mis- or malfeasance;
- keeping vacant sensitive areas locked, subject to periodic inspection, and/or monitored remotely as appropriate by video or other technologies; and
- limiting video, audio or other recording equipment, including cameras in portable devices, in sensitive areas.

Public access, delivery, and loading areas

Public access, delivery and loading access • In Cogent E Services access points such as delivery and loading areas, and other points where unauthorized persons may enter the premises, should be controlled. This could include:

- limits on access to the delivery and loading areas, and to other public access areas, to the degree consistent with required operations;
- inspection of incoming and outgoing materials, and separation of incoming and outgoing shipments, where possible; and
- Isolation of these areas from information processing facilities and areas where information is stored, where possible.

EQUIPMENT SECURITY

Equipment siting and protection

Equipment siting and protection • In Cogent E Services equipment should be sited and protected to reduce the risks from environmental threats and hazards, and to reduce the opportunities for unauthorized access by human threats. This could include siting:

- to minimize unnecessary risks to the equipment, and to reduce the need for unauthorized access to sensitive areas;
- to isolate items requiring special protection, to minimize the general level of protection required;
- with particularized controls as appropriate to minimize physical threats -- e.g., theft or damage from vandalism, fire, water, dust, smoke, vibration, electrical supply variance, or electromagnetic radiation; and
- Guidelines for eating, drinking, smoking or other activities in the vicinity of equipment.

Supporting utilities

Supporting utilities • Equipment should be protected from power failures, telecommunications failures, and other disruptions caused by failures in supporting utilities such as HVAC, water supply and sewage. This could include:

- assuring that the supporting utilities are adequate to support the equipment under normal operating conditions; and
- Making reasonable provision for redundant equipment and backups (e.g., a UPS) in the event of supporting utility failure.

Cabling security

Cabling security • Power and telecommunications cabling carrying sensitive data or supporting information services should be protected from interception or damage. This could include:

- physical measures to prevent unauthorized interception or damage, including additional protections for sensitive or critical systems;
- alternate/backup routings or transmission media where appropriate, particularly for critical systems;
- clearly identified cable and equipment markings, except where security is enhanced by removing/hiding such markings; and
- Documentation of patches and other maintenance activities.

Equipment maintenance

Equipment maintenance • Equipment should be correctly maintained to ensure its continued availability and integrity. This could include:
appropriate preventive maintenance, as specified by the manufacturer or regulatory-certificatory authorities;

- documentation of all maintenance activities, including scheduled preventive maintenance;
- documentation of all suspected or actual faults, and associated remediation, in accordance with an incident management policy;
- maintenance only by authorized, certified employees or contracted third parties; and
- Appropriate security measures, such as clearing of information or supervision of maintenance processes, appropriate to the sensitivity of the information on or accessible by the devices being maintained.

Security of equipment off-premises

Security of property off-premises • In Cogent E Services appropriate security measures should be applied to off-site equipment, taking into account the different risks of working outside Cogent E Services premises. This could include:

- authorization of any off-site processing of organizational information, regardless of the ownership of the processing device(s);
- security controls for equipment in transit and in off-site premises, appropriate to the setting and the sensitivity of the information on or accessible by the device;
- adequate insurance coverage, where third-party insurance is cost-effective; and
- Employee and contractor awareness of their responsibilities for protecting information and the devices themselves, and of the particular risks of off-premises environments.

Secure disposal or re-use of equipment

Secure disposal or re-use of property • In Cogent E Services all equipment containing storage media, and independent storage media devices, should be checked to ensure that sensitive data and licensed software has been removed or securely overwritten prior to disposal. This could include:

- use of generally accepted methods for secure information removal, appropriate to the sensitivity of the information known or believed to be on the media; and
- secure information removal by appropriately trained personnel, or verification of secure information removal by appropriately trained personnel.

Removal of property

Removal of property to off-premises locations • In Cogent E Services equipment, information or software should not be take off-premises without prior authorization and subject to appropriate restrictions. This could include:

- limitations on types or amounts of information, or types of equipment, that may be taken off-site;
- recording of off-site authorizations and inventory of equipment and information taken off-site; and
- for persons authorized to take equipment or information off-site, appropriate awareness of security risks associated with off-premises environments and training in appropriate controls and counter-measures.

SECTION 3 – STAKEHOLDER - ROLES AND RESPONSIBILITIES

STAKEHOLDER

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

Stakeholder	Roles & Responsibility
	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 Security Steering Committee .Performs the audit using the consolidated audit checklist. ▪ Reports the non-conformities and

Stakeholder	Roles & Responsibility
	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	Chief Information Security Officer
Consulted	ISWG
Informed	ISSC

SECTION 4 – PERFORMANCE MEASURES

CRITICAL SUCCESS FACTORS:

S. No.	Critical Success Factors
1	Adherence to Procedure by all concerned
2	Effective & Timely Internal Audits
3	Top Management Support & Commitment
4	Regular Management Reviews
5	Competence of Internal Auditors
6	Independence of Internal Auditors

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 Chief 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

SECTION 7 – APPENDIX

APPLICABLE FORMATS

END OF DOCUMENT