ANTIVIRUS 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 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 ANTIVIRUS POLICY

1.0 Overview

This policy is an internal IT policy which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

2.0 Purpose

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

3.0 Anti-Virus Policy

The organization will use a single anti-virus product for anti-virus protection and that product is Symantec endpoint Protection manager and MacAfee. The following minimum requirements shall remain in force.

1. The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.
2. The anti-virus library definitions shall be updated at least once per day.
3. Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

4.0 Email Server Policy

The email server will have additional protection against malware since email with malware must be prevented from entering the network.

4.1 Email Malware Scanning

In addition to having the standard anti-virus program, the email server or proxy server will

additionally include protection which will be used to scan all email for viruses and/or malware. This scanner will scan all email as it enters the server and scan all email before it leaves the server. In addition, the scanner may scan all stored email once per week for viruses or malware.

When a virus is found or malware is found, the policy shall be to delete the email and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. It would simply cause an additional help desk call by the notified person and most likely waste system administrator's time needlessly. Notifying the recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of help desk calls.

Do not depend on your anti-virus software on each computer to prevent these viruses. Viruses have a period of time when they spread unrecognized by anti-virus software. Blocking these file attachments will prevent many trouble calls. Give the users a work around for your network to get some of their files sent to other organizations. Your solution will depend on your network and the software that is being used to block the file attachments. In one case we renamed the file to another type and instructed the recipient to rename it back to the original name before using it. This will not work in all cases since some file blocking software senses the actual file type regardless of its named file extension.

When an email breaks the rules and contains an illegal file attachment your policy should define one of the following to be done:

- Delete the email and notify neither the sender nor the recipient. The problem with doing this is in the fact that people may be trying to send legitimate files to each other and have no way of knowing their communication attempts are failing. Training by letting users know what files are blocked can help remedy this problem
- Delete the email and notify the sender - This will notify senders when their emails do not go through, but it will also notify senders who really did not send an email (when a virus spoofed them as the sender) that they sent an email with an illegal attachment.

This can cause more additional help desk requests and questions for the administrator on the spoofed sender's side.

- Delete the email and notify the sender and recipient. - This would have all the drawbacks of the above policy but would also increase help desk calls in your organization.
- Remove the attachment and let the email go through. - This would let the receiver know that someone tried to send them an illegal attachment. If the attempt was a legitimate one, they could contact the sender and tell them what to do to get the attachment sent. This policy would very likely cause your organization's help desk calls to increase with users calling to ask questions about why someone is trying to send them these files.

SECTION 3 – STAKEHOLDER - ROLES AND RESPONSIBILITIES

STAKEHOLDER

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

Stakeholder	Roles & Responsibility
	▪ 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 recommends suggestions for improvement

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

RACI MATRIX

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

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

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

SECTION 4 – PERFORMANCE MEASURES

CRITICAL SUCCESS FACTORS:

S. No.	Critical Success Factors
1	Top Management Support & Commitment
2	Adherence to Procedure by all concerned
3	Regular Monitoring and Measurement.
4	Regular Management Reviews

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

END OF DOCUMENT