Cogent E Services Private Limited

Guidelines on Acceptable Use of Assets

Based on ISO/IEC 27001:2013

Version: 3.2

Corporate Information Security Guidelines

Preface

The Cogent E Services Private Limited (hereafter referred to as "Cogent") Information Security Management System (ISMS) Team assumes responsibility for this document and updates it as required to meet the needs of users. The Cogent 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. It will be maintained by the Information Security Manager (ISM) and is subjected to review at a minimum on a yearly basis.

Document Revision 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	

Copyright

Document Distribution

The Cogent Chief Information Security Officer (CISO) shall distribute this document to members of Information Security Steering Committee (hereafter referred to as ISSC) and

Information Security Implementation Committee (hereafter referred to as ISIC).

The softcopy of the manual and related documents will be accessible to all employees in read-only mode through intranet server at location http://*********

The CISO will ensure that any update to the Cogent ISMS is incorporated on the intranet server and is communicated to all employees of Cogent through an appropriate mode such as e-mail.

Distribution List

Name	Acronym
Information Security Steering Committee	ISSC
Information Security Implementation Committee	ISIC
Chief Information Security Officer	CISO
All employees and relevant external parties.	-

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.

Table of Contents

1 Objective

To create awareness among users of Cogent E Services Private Limited (hereafter referred to as "Cogent") information assets, about their responsibilities towards security of Cogent information and information processing devices.

2 Scope

This guideline documents the security related responsibilities of Cogent personnel and users of information resources.

3 Applicability

These guideline procedures apply to all users of information assets of Cogent including employees, vendors, business partners, and contractor personnel.

4 Acceptable Use Policy

4.1 Usage of Cogent Information Systems

4.1.1 Usage of information systems and resources for personal usage or on behalf of a third party (i.e., personal client, family member, political or religious or charitable or school organization, etc.) is strictly prohibited.

4.1.2 Usages of information systems to store, process, download, or transmit data that can be constructed as biased (politically, religiously, racially, ethnically, etc.) or supportive of harassment is strictly prohibited.

4.1.3 Downloading, redistribution and printing of copyrighted articles, documents, to Cogent information systems are strictly prohibited.

4.1.4 Receiving, printing, transmitting, or otherwise disseminating proprietary data, company secrets, or other confidential information in violation of company policy or proprietary agreements is strictly prohibited.

4.1.5 Users should terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

4.1.6 Users are prohibited from changing the configuration of, removing, de-activation or otherwise tampering with any Virus and Malicious Software prevention / detection and software that has been installed on systems used by them.

4.2 Prohibiting Usage of Unauthorized Copies of Licensed Software & Hardware

4.2.1 Introduction of unauthorized copies of licensed software & hardware (piracy/copyright & patent infringement) to Cogent information resources and the copying of such material is prohibited.

4.2.2 The storage, processing, or transmission of unauthorized copies of licensed software & hardware (piracy/copyright & patent infringement), by Cogent personnel is strictly prohibited.

4.3 Introduction of Open-source, Freeware and Shareware Applications

4.3.1 Introduction of Open-source, Freeware and Shareware Applications whether downloaded from the Internet or obtained through any other media to Cogent information systems will be subject to a formal evaluation and approval process by Head - IT & CISO.

4.4 Introduction of Pornographic Material

4.4.1 The introduction, storage, processing, or transmission of pornographic material on Cogent information systems, by Cogent employees, contractors or associates is strictly prohibited.

4.5 Due Diligence

4.5.1 Each user has the responsibility to notify the Head – Information Security & Head - Administration immediately of any evidence of or suspicion of any security violation with regard to:

4.5.1.1 Unauthorized access to network, telecommunications, or computer systems;

4.5.1.2 The apparent presence of a virus on a PC;

4.5.1.3 The apparent presence of any information resource prohibited by this policy;

4.5.1.4 Apparent tampering with any file for which the user established restrictive discretionary access controls; and

4.5.2 Violation of this Policy or any other Information Security policy or procedure by another user, employee, contractor or third party service provider.

4.5.3 Each user has the responsibility to prevent unauthorized access, including viewing, of information resources in his possession or control (such as portable computer or desktop terminal/computer or printouts or floppy/tape media).

4.5.4 Each user is responsible for providing security access against relatives, friends & neighbors, customers/clients, vendors, and unknown visitors. In situations where such people should be provided access (e.g., a vendor who has come to install a product or make repairs), then the user should oversee and monitor the actions of the individual given temporary access.

4.6 Computer Games

4.6.1 Playing computer games in Cogent premises is prohibited during office hours. Users should not install any computer games (except default operating system games) in Cogent information resources.

4.7 Introduction of Destructive Programs

4.7.1 Introduction of destructive programs (e.g., viruses, self-replicating code) in order to do intentional damage, interfere with others, gain unauthorized access, or inhibit production to Cogent information systems, is strictly prohibited.

4.8 External Services

4.8.1 All users should limit their usage of external services (e.g., bulletin board, on-line service provider, Internet site, commercial data base) to authorized business purposes only in accordance with this policy, standards, and procedures regarding such usage and as approved by the user's management.

5 Physical Security

5.1 Building planning and materials security and guarding standards

5.1.1 Procedures for guarding in accordance with the sensitivity of the asset involved have been put in place. procedures for guarding in accordance with the sensitivity of the asset involved have been put in place All controlled access points should have Antipas back access control system reinforced by camera surveillance and 24x7 security guards posted at all entry and exit points. Facilities have been equipped with Fire alarm systems that are tested on a regular basis the buildings where the business operations are being carried out have been certified by the relevant fire departments as well.

5.2 Insurance protection

5.2.1 Where possible and if financial prudence permits assets should be safeguarded by procuring insurance. To avoid denial of insurance claims by breach of any of the insurance contracts. We must act in a disciplined and responsible manner and at all times use our assets in a prudent manner. Cogent has amongst others procured insurance directly or indirectly to protect against the following perils.

5.2.1.1 Burglary

5.2.1.2 Fire

5.2.1.3 Loss of Profit

5.2.1.4 Professional Indemnity

5.2.1.5 Public Liability

5.3 Recommendations for Secure Environment

5.3.1 All users are advised to follow the below listed recommendations to provide for a safe and secure environment.

5.3.2 Users should not allow any unauthorized person to enter Cogent .

5.3.3 Users should not enter into Cogent without ID badges and they should always display their ID badges with in Cogent .

5.3.4 Users should disclose and declare voluntarily all their belongings while entering and going out of Cogent to the security personnel.

5.3.5 Users are prohibited from carrying large bags into Cogent premises; only small handbags will be allowed, and all personal belongings will be subject to search by security.

5.3.6 Smoking, drinking or eating is strictly prohibited inside Cogent .

5.3.7 Users should not take in or out any equipment from Cogent , without authorization (This includes Floppies, CD, USB/Pen drive, Digital cameras and Laptop/PDA which are declared on the declaration form).

5.3.8 To further strengthen the security mechanism and ensure surveillance of all visitors and employees closed circuit televisions should be installed on Cogent facilities. This camera's record on a 24X7 basis. Camera surveillance is used for visual monitoring of main doors. Visual monitoring and recording system are under access control and are not accessible to the public.

5.4 In view of the determined security levels

5.4.1 All verbal communication should be avoided in public areas, conference rooms must be used. Written transfer of information must be clearly marked as confidential or personal. Electronic Access Control system should be used. Entry doors must be equipped with card readers. Video surveillance system must be used for additional security. Emergency exits should be secured using security guards

5.5 Equipment Sitting and Protection

5.5.1 Equipment should be sited to minimize unnecessary access into work areas.

5.5.2 Information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access.

5.5.3 All mechanical assets should be accessed only on a need basis and appropriate records/approvals are maintained. All Electromechanical assets should be accessed only on a need basis and after appropriate records/approvals of the same are obtained

5.5.4 Controls should be adopted to minimize the risk of potential physical threats, e.g., theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.

5.5.5 Environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information processing facilities.

6 Handling Confidential Information

1. Confidential/restricted information should always be transmitted through trusted communication links not through public networks.
2. Confidential information stored or transported in computer-readable storage media (such as magnetic tapes, floppy disks or CDs) should be appropriately protected from the reach of unauthorized individuals.

7 Use of Office equipment

7.1 Telephone

7.1.1 Staff should not reveal sensitive or classified information over the telephone unless the telephone lines have been specifically secured for this purpose – for example through the use of encryption.

7.1.2 Staff should not enter into the conversation or reveal any information to over the telephone where the identity of the caller cannot be determined.

7.1.3 Where appropriate, staff should confirm telephone conversations by creating signing and acknowledging a formal written transcript of the conversation.

7.1.4 Staff should not discuss confidential matters or reveal confidential / classified information in public places and / or outside Cogent premises.

7.1.5 Staff should not reveal or store confidential messages on answering machines or voice-mail services.

7.1.6 All parties on a telephone call should be notified in advance if the call is to be recorded.

7.2 Fax Machines

7.2.1 Sensitive or confidential information should be faxed only, when a more secure means of communication is not available. Both the sender of the information and the intended recipient should authorize the transmission of the information before the transmission.

7.2.2 All fax messages should be classified as per Asset Classification guidelines and should be handled accordingly.

7.2.3 Users should not leave the fax messages near the fax machine or near desktops unattended.

7.2.4 Any fax received in error should be destroyed and its sender notified, wherever possible.

8 Internet

8.1 Implied restrictions on Internet

8.1.2 Users using Cogent computers on discovering that they have connected with a web site that contains potentially offensive material should immediately disconnect from that site.

8.1.3 Users should be aware that Cogent accepts no liability for the exposure to offensive material that they may access via the Internet.

8.1.4 The ability to connect with a specific web site does not in itself imply that users of Cogent systems are permitted to visit that site.

8.2 Management Review

8.2.1 At any time and without prior notice, Cogent management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, and other information stored on or passing through the company's computers. All transactions done over the Internet will be logged. These logged transactions will be used for analysis and can be audited.

8.3 Restrictions on Posting Cogent Material

8.3.1 Users should not place the company's information or material (software, internal memos, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar services, unless the CTO has first approved the posting of these materials.

8.4 E-Mail

8.4.1 Each employee is responsible for the contents of his/her e-mail and all actions performed using his/her email logon credentials.

8.4.2 Email should be used only for business purposes. Personal or non-business use of the information systems is not permitted.

8.4.3 Only the email client authorized for use by Cogent management should be used.

8.4.4 Users should use only their own official E-Mail account and should not allow anyone else to access their email account. Users should identify themselves by their real name; pseudonyms that are not readily attributable to actual users should not be allowed. Users should not represent themselves as another user. Each user should take precautions to prevent unauthorized use of the E-Mail account. Forging of header information in E-Mail (including source address, destination address, and timestamps) is not permitted.

8.4.5 Users should not provide other unauthorized persons with their E-Mail ID and password.

8.4.6 Users should not send any information about Cogent to any other person without confirming the identity of the person through other means.

8.4.7 Users should not subscribe to any forums using company email account without verifying the reputation and the purpose of the forum. Users should not post any company related information to any forums using company mail account.

8.4.8 Users should compress all attachments prior to sending emails.

8.4.9 E-mail should not be used to transmit or receive statements that contain any material that is offensive, defamatory, or threatening to others.

8.4.10 Employees may either communicate with the originator of the offensive E-mails, asking him/her to stop sending such messages, or report such offensive E-mails directly to Head – Information Security.

8.4.11 Users should not post network or server configuration information about any Cogent machines to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, or software version numbers.

8.4.12 Users who cannot access their email for long periods (due to vacation, outstation work, etc.) should use "Out of Office" feature in the email system to make aware of the sender that the recipient is out of office.

8.4.13 Users must not employ a scanned version of a hand-rendered signature to give the impression that the sender signed an E-mail message or other electronic communications, as another person could misuse the signature.

8.4.14 Users should not modify the security parameters within Cogent E-Mail system. Users making unauthorized changes to the E-Mail security parameters are in violation of this policy.

8.4.15 Users should not send unsolicited bulk mail messages (also known as "junk mail" or "spam"). This practice includes, but is not limited to, bulk mailing of commercial advertising and religious or political tracts. Malicious E-Mail, including but not limited to "mail bombing," is prohibited.

8.4.16 At any time, with or without notice, this information may be monitored, searched, reviewed, disclosed, or intercepted by Cogent for any legitimate purpose, including the following:

8.4.16.1 To monitor performance,

8.4.16.2 Ensure compliance with Cogent policies,

8.4.16.3 Prevent misuse of the Systems,

8.4.16.4 Troubleshoot hardware and software problems,

8.4.16.5 Comply with legal and regulatory requests for information, and

8.4.16.6 Investigate disclosure of confidential business, proprietary information, or conduct that may be illegal or adversely affect Cogent or its associates.

9 Virus Protection

1) Users should not open any files attached to an email from an unknown, suspicious or untrustworthy source. Users should not open any files attached to an email whose subject line is questionable or unexpected. If there is a need to do so, they should always save the file to the hard drive before doing so.
2) Users should not open attachments that are from an unknown or non-trusted source. Attachments with extensions such as '.exe', '.vbs', etc should be blocked by the anti-virus engine.
3) Users should delete chain/junk emails and not forward or reply to any of the chain/junk mails. These types of email are considered Spam, which is unsolicited and intrusive that clogs up the network.
4) Users should exercise caution when downloading files from the Internet, and should download only from a legitimate and reputable source. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.
5) Users should back up the files on a regular basis. If a virus destroys the data files, they can be replaced with the back-up copy. The backup files should be stored in an off-site location.
6) When in doubt, always err on the side of caution and do not open, download, or execute any files or email attachments.

1. Assimilate Solutions explicitly defines the unacceptable behavior and usage of its IT resources. Any unacceptable usage identified results in initiation of disciplinary action against the concerned user.

2. All the users including employees, business partners and third party vendors are briefed about the acceptable usage of the information resources during induction training.

3. All the users including employees, business partners and third party vendors are briefed about the acceptable usage of the information resources before being granted access.

4. For security and network maintenance purposes, authorized individuals within RGUH may monitor equipment, systems and network traffic at any time.

5. Management reserves the right to audit information assets including information processing facilities on a periodic basis to ensure compliance with this policy.

10 Asset Use Procedures

10.1 On Induction

a) The employee shall ensure that he/she attends the Information Security Training given to the employees on induction.

b) The employee shall read and understand the Information Security Management System of the organization.
c) The employee shall familiarize him/herself with the ways and means to access the information security policies and procedures.
d) The employee shall undertake to abide by all the Information security policies and procedures of the organization.

10.2 During Employment

a) Desktop and laptop computers are for official purpose and shall be used for business purposes only.

b) Users shall use only reasonable amount of storage on their desktop computers or laptops to store their personal files/data.

c) Users shall not use any Network location to store their personal files/data.

d) Users shall use the canteen/cafeteria facility for the purpose of consuming eatables and shall avoid consuming eatables on or near their work area.

e) Users shall install only authorized and approved software on their computer systems. CISO shall be responsible for approving any such software on business requirement.

f) The employee shall not use Cogent facilities for profit making or commercial activity.

10.3 Internet Usage

a) Internet connectivity shall be used for official purpose only and shall be driven by the business need.

b) Subscription to any news group or Bulletin board will be allowed on a need basis

c) While posting any comment on the Internet newsgroups or on the Internet bulletin boards, employees of Cogent must clearly state that the opinions expressed are their own and cannot be related to Assimilate Solutions.

d) Users shall subscribe to only those newsgroups, which are approved by the Information Security Management Forum/CISO.

e) IT department is responsible for identifying and blocking all the web sites having contents purported to be obscene, racial, and sexual or in any inappropriate and indecent.

f) Users shall not download/install any file or software from the Internet. A list of approved sources to download files/software shall be prepared and maintained by IT department and approved jointly by CISO and Information Security Management Forum. Any software/tool required to be installed for evaluation will be downloaded by the IT department and its usage period will be tracked. Post expiry, the same will be removed from the systems

10.4 Email Usage

a) Email is provided to all the users in office on the recommendation of the Head of the Department or Manager.

b) Assimilate Solutions email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender,

disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

c) Internal mails as well as mails to business partners and third party vendors shall be sent using official e-mail accounts only. Employees shall include their full name, designation, department and location in the 'signatures' to be appended to each e-mail.

d) Confidential Information must not be sent by email in open text format. Encryption mechanism must be used to protect the disclosure of confidentiality.

e) Using a reasonable amount of Cogent resources for personal emails is acceptable, but non-work related email must not be saved. Employees shall not use official e-mail accounts for sending and receiving personal e-mail messages.

f) Sending chain letters or joke emails from Cogent email account is prohibited. Users shall not create or forward chain letters, or mails that can be deemed to be spam/junk, using their official e-mail account.

g) Monitoring: Cogent employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Cogent may monitor messages without prior notice.

h) Enforcement: Employees must be aware of this policy and must adhere to it. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10.5 Physical Security

a) The employee shall prominently display their ID cards whenever they are in the Company premises.

b) The employee shall ensure that no unauthorized person enters a working area behind him/her.

c) The employee shall entertain the visitors only by prior appointments

d) The employee shall escort his visitors from and to the reception area

10.6 Network Security

a) The employee shall access the Cogent network only if authorized by an appropriate login and password.

b) The employee shall not share his/her login and password with anybody unless specifically approved.

c) The employee shall not allow another person to obtain unauthorized access to an information asset by using his/ her right of access.

d) The employee shall ensure that a password protected screen saver and/or NT/2000/XP desktop locking mechanism is activated when the workstation is unattended.

e) The employee shall not use any non-standard screensavers, wallpapers, freeware or Shareware.

f) The employee shall not post any information related to Cogent on the internet unless duly permitted by HOD. Postings by employees from Cogent email address to newsgroups shall contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Assimilate Solutions, unless posting is in the course of business duties.

g) It shall be mandatory for the employee to log off the computer at the conclusion of the work period.

h) The employee shall be careful while using any outside media devices such as floppy disks, CDs etc. in the Organization. The media shall be scanned for viruses before opening them for use.

i) The Employee shall use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

j) The employee shall not install or keep/dump their personally owned software on Company equipment.

k) The employee shall not make unauthorized copies of the software purchased by Assimilate Solutions.

l) The employee shall not make unauthorized copies of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Cogent or the end user does not have an active license.

m) The employee shall not engage in procuring or transmitting material, which is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction, using Cogent information processing facilities.

n) The employee shall avoid indulging in personal surfing during working hours.

o) None of the employee of Assimilate Solutions, under any circumstances, shall engage in any activities that are alleged to be illegal under local, state, or international law while utilizing company owned resources.

p) None of the employee of Assimilate Solutions, under any circumstances, shall violate the rights by any person or company, protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations. This includes the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Assimilate Solutions.

q) Unauthorized copying of copyrighted material and the installation of any copyrighted software for which Cogent or the end user does not have an active license, shall be strictly prohibited.

r) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management shall be consulted prior to export of any material that is in question.

s) The employee shall not introduce any malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

t) The employee shall not reveal one's account password to others or allowing use of one's account by others. This includes family and other household members when work is being done at home.

u) The display of any kind of sexually explicit image or document on any Cogent system shall be a violation of Cogent IT Security policy as well as the IT Act 2000.

v) Making fraudulent offers of products, items, or services originating from any Cogent email account.

w) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data to which the employee is not an intended recipient or logging into a server or account that the employee shall not be expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but shall not be limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

x) Port scanning or security scanning shall be expressly prohibited, except for the IT Department when authorized by the CISO.

y) Executing any form of network monitoring which shall intercept data not intended for the employee's host, unless this activity shall be a part of the employee's normal job/duty.

z) Providing information about, or lists of, Cogent employees to parties outside Assimilate Solutions.

10.7 Incident Reporting & Handling

a) The employee shall promptly advise their immediate supervisor/senior, if they discover that someone is placing the performance or security of any information asset at risk.

b) The employee shall promptly report all the information security incidents to the relevant personnel.

10.8 Traveling

a) The employee shall store all the confidential information securely while traveling.

b) The employee shall avoid accessing/working on confidential information while traveling. (Public places like airports etc)

c) The employee shall carry all the confidential information in their handbags and not check-in baggage.

d) The employee shall ensure that the documents they are studying/drafting cannot be viewed by anyone else.

e) The employee shall ensure that the hard disk of their laptop is encrypted while they are traveling.

f) The employee shall not talk about confidential information relating to business with co-passengers.

g) The employee shall ensure that their conversation on the cell-phone is not overheard.

h) The employee shall not share the dial-up telephone number, access username and password used for connecting to the office network from outside with anybody.

10.9 Mobile Computing Devices

a) The employee shall take appropriate care while using the mobile computing devices allotted to them by the organization.

b) All the employees, who use Laptops, shall use Laptop locking devices provided by IT department to physically secure their laptops. The Laptops shall be locked at all times especially when they are unattended.

c) The employee shall never leave their PDAs, Cellular Phones, Digital diaries, USB Drives etc. unattended.

d) The employee shall use power on password for their mobile computing devices.

10.10 Hardware & Software Controls

Hardware Equipment

Equipment maintained by Cogent must not be altered or enhanced without the authorization of CISO, whether by users or by authorized third-party vendors under a maintenance and/or technical support agreement.

Operating Systems Configuration

Users are not permitted to change operating system configurations, upgrade existing operating systems, apply patches or install new operating systems on Cogent -owned equipment. If such changes are required, they are performed by Cogent IT Department only.

11 Related Documents

2.1. ISMS L2-A8:Asset Management Policy and Procedure