COGENT

Cogent E Services Private Limited

Information Security Policy

Based on ISO/IEC 27001:2013

Version: 3.2

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	22nd Dec’20	CISO	22nd Dec’20	ISSC	22nd Dec’20	3rd Jan’21	
3.2	ISM	07 Apr’22	CISO	07 Apr’22	ISSC	07 Apr’22	11th Apr’22	

Copyright

This document contains proprietary information for Cogent. It may not be copied, transferred, shared in any form by any agency or personnel except for authorized internal distribution by Cogent, unless expressly authorized by Cogent Information Security Steering Committee in writing.

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

Introduction

The confidentiality, integrity and availability of information are of great importance to the operation and administration of Cogent. Failure in any of these areas can result in disruption to the services that Cogent provide as well loss in confidence in the employees and organisations investing in Cogent. The security of our information and other assets is therefore regarded as fundamental to the successful operation of Cogent.

Policy Statement

Cogent E Services Private Limited

(hereafter referred to as "Cogent")

INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

"Information security and its demonstration to our existing and prospective clients is critical to our survival and key to our growth.

Cogent shall use ISO 27001:2013 and its requirements as an Information Risk Management Framework to create its own Information Security Management System (ISMS).

Information security risk management will form a key component of all our processes and functions and ownership of managing risks of the assets shall rest with the asset owner.

Cogent shall implement procedures and controls at all levels to protect the Integrity, Confidentiality and Availability of information stored and processed on its systems and ensure that information is available to authorized persons as and when required.

Cogent is committed to continual improvement of its information security management system based on ISO/IEC 27001:2013 while meeting all legal, statutory and regulatory requirements.

Sd/-
ABHINAV SINGH
MANAGING DIRECTOR
5th April 2015. Version 2.0

Applicability

This policy applies to:

- All employees, staff and visitors to Cogent
- All information assets owned or managed by Cogent
- Access rights and controls to information
- Security of services and information systems
- Business continuity and disaster recovery of information
- Appropriate controls to meet statutory, regulatory and legal requirements
- Framework for third parties and employees to adhere to
- Promotion of security and guidance and advice where appropriate
- Processes to prevent and deal with security breaches

Cogent ISMS Scope

Cogent has determined the boundaries and applicability of the information security management system to establish its scope.

"The management of information security applies to BPO operations and the support functions of IT, Software development, Data services, HR & Training, Quality, Administration, Finance and Legal, at its Corporate office at Noida Sec- 63, C-100 and site office at Noida Sec 63, C-121. This is in accordance with the statement of applicability dated January 1st, 2015 Version 1.0".

Management Commitment

Cogent is committed to building and maintaining long term business relationships with our customers and partners. Recognizing the value of all information assets including those of our customers, partners and suppliers, we will establish an Information Security Management System to maintain the trust and confidence of all stakeholders. We will maintain and enhance our corporate ethics efforts concerning legal compliance and business continuity to ensure the integrity and trustworthiness of our role in the global information society.

Cogent management is committed to ensure security of Organizational Information Assets including data of all business partners associated with it through the effective functioning and Continual Improvement of its ISMS. We shall ensure that appropriate information security controls are applied and integrated to ensure information protection from threats to confidentiality, integrity and availability thereby enhancing confidence of and adding value to all its stakeholders. This will be continuously monitored to ensure compliance at all levels of the organization.

It is Cogent's policy to:

- ensure that information is accessible only to those authorised to have access;
- safeguard the accuracy and completeness of information and processing methods;
- ensure that authorised users have access to information and associated assets when required;
- ensure that information it manages shall be secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information;
- define an information classification scheme describing classes and how information of a particular class should be managed (stored, accessed, transmitted, shared, and disposed of);

- meet all information security requirements under appropriate regulations, legislation, organisation policies and contractual obligations;
- address the security of all of our services and processes to ensure that risks are identified and appropriate controls are implemented and documented;
- provide a secure operational environment for staff ;
- Information security education, awareness and training will be made available to the employees. Promote this policy and raise awareness of information security throughout the office; provide appropriate information security training for our employees and staff;
- Business continuity plans are produced, maintained and tested as far as practicable.
- All breaches of information security, actual or suspected, will be reported to, and investigated by the relevant authorities.
- Information Security Management System shall be managed through a Risk Management framework.
- Contractual, Regulatory and legislative requirements will always be met.

Adherence to this policy will help to protect Cogent and its employees from information security threats, whether internal or external, deliberate or accidental. We are committed to good information security provision for customers and for our employees

Responsibilities

Within this policy, the following individuals have the following responsibilities:

Responsibility	Owner
• Sponsor of this policy	Managing Director
• Publish, support and review this policy. • Execution and Quality Assurance of this policy.	Chief Information Security Officer (CISO)
• Production, maintenance, controls and guidance of this policy and writing and/or managing the development of relevant policies, procedures and guidelines for supporting information security.	Information Security Steering Committee (ISSC)
• Ensuring employees have an awareness of and put appropriate controls in place to adhere to the policy • The Information Security Manager facilitates the implementation of this policy through the appropriate standards and procedures.	Information Security Manager (Cogent CISO)
• Protection of information systems and assurance that security processes and controls have been carried out. All business unit heads/managers/policy owners are directly responsible for implementing the Cogent ISMS Policy within their section/department/division and for adherence by their employees.	Respective Process Managers

Responsibility	Owner
• Initiation, co-ordination and investigation of potential breaches in policy	Information Security Implementation Committee (ISIC)
• Provide advice, guidance, training and support on information security to the Organisation	Information Security Manager
• Adherence to policy and reporting security incidents and any identified weaknesses.	All employees, staff contractors and visitors

Information Security Objectives

Our Information Security Goals are listed below:

- Protection of Customer information.
- Protection of information assets belonging to Cogent
- To provide confidence to trading partners where information needs to be shared.

The specific Information Security Objectives of Cogent are:

1) To develop an effective **Information Security Management System** (Cogent ISMS)
2) To identify the **value of information assets**, to understand their vulnerabilities and the threats that may expose them to risk, through **appropriate risk assessment** maintaining confidentiality, integrity and availability of information**.**
3) To **Handling information appropriately** and according to its data classification
4) To **manage the identified risks** to an acceptable level through the design, implementation and maintenance of a formal Information Security Management System.
5) To **comply with applicable laws and regulations** pertaining to information security, be it for its own data or customer data held by Cogent.
6) To comply with any additional **customer specific information security requirements** relating to information security.
7) To **prevent disruption to work** being undertaken within operation and support services that lead to financial loss or loss of reputation to Cogent.
8) To produce, maintain and test **Business Continuity / Disaster Recovery** Plans as applicable by managing and minimizing the impact of information security incidents.
9) To **raise awareness** of the security risks with information and information systems.
10) To implement mechanisms to ensure that all **breaches of information security** and suspected weaknesses are reported and investigated followed by adequate action.
11) **Transition existing Cogent ISMS** and obtain its certification to ISO 27001:2013 for our Cogent ISMS without any significant non conformances
12) To **continually analyse, review** and **manage our information security risks** and **report on the performance of the control measurements**
13) Encourage departments to **use the near miss area** to highlight potential security incidents
14) To **implement continual improvements** to the Information Security Management of Cogent
15) To Make **information security a culture** in Cogent

These policy objectives are achieved through the implementation of our Information Security Management System, which includes security standards, procedures and guidelines developed in accordance with ISO/IEC 27001:2013.

Review

- This Information Security policy will be reviewed every 12 months or sooner as necessary by the Information Security Council to ensure that it remains current in the light of relevant legislation, organisational procedures or contractual obligations. Changes will be approved by the Managing Director of Cogent.

Note:

- This Cogent ISMS Policy is approved by Cogent ISSC and is issued on a version controlled basis.
- Policies, Procedures and Guidelines for Information Security in Cogent will be made available in both hardcopy and electronic format to support the Cogent ISMS Policy.
- Any deliberate act to jeopardize the security of information that is the property of Cogent or their customer or suppliers will be subject to disciplinary and/or legal action as appropriate.

Policy framework based on Annexure A Controls

5. Information Security Policy

Control objective: The organisation provides management direction and support for information security in accordance with business requirements and relevant laws and regulations

5.1 Information security policy document

The management team and the Board of Directors have approved and authorised an information security policy for Cogent . This policy is set out in the **Corporate IS Policy** and is authorised for separate distribution under the **Managing Director's signature**. A current version of this document is available to all staff and contractors on the corporate intranet a copy are also available at all points of use, and to external parties when signing supply contracts.

5.2 Review of the information security policy

Cogent information security policies are reviewed at planned intervals, or when and if significant changes occur, to ensure their continuing suitability, adequacy, and effectiveness.

- The **CISO** is the Owner of the information security policies and has approved management responsibility for the development, review and evaluation of the policies.

- Cogent has a defined procedure (**Management Review of Information Security Procedure**) for the management review of the information security policies, and this includes continual improvement, and assessing policy changes that might be necessary in response to significant changes in the organisational environment, business circumstances, legal conditions, technical environment or requirements of interested parties.

- All changes to the information security policy are subject to approval by Cogent's board.

6. Organisation of Information Security

6.1 Internal Organisation

Control objective: establishment of a management framework for the initiation, implementation and operation of information security within the organisation.

6.1.1 Information security roles and responsibilities

Cogent has clearly defined and allocated all information security responsibilities.

- Responsibilities for specific information security procedures are clearly defined throughout the Cogent ISMS , and are documented in individual job descriptions.

- The **Head of HR** is responsible for ensuring that Cogent has standard job descriptions for all roles, that contain defined security roles and responsibilities, and that these apply to all users of organisational information assets. Job descriptions are provided to all prospective users prior to their recruitment.

- The **CISO / Head of HR is** responsible for ensuring that information security and IT staff have specific information security responsibilities and that these are detailed in their job descriptions.

- The **Head of HR** and the Manager/Executive is responsible for ensuring that all users sign User Agreements (see 9.2 below) before they are allowed to access Organisational information assets; these User Agreements contain specific information security responsibilities.

- The **CISO**, who has lead responsibility in the management team for information security, is responsible for the development, implementation and maintenance of the Cogent ISMS .

- The **Information Security Team** reports to the **CISO.**

- The **Information Security Team Members'** responsibilities are documented in his/her job description and include the day-to-day responsibility for the implementation, co- ordination and maintenance of the Cogent ISMS.

- All staff (and certain third party contractors) have accepted their specific responsibilities in the User Agreements which they sign before they are authorised to access organisational information assets.

- All information assets have been identified (see 8.1.1 below) and the security processes associated with each asset have been defined following a risk assessment (**Risk Management Methodology**) and documented on the asset inventory schedules (see section 8.1 below).

- All assets have identified Owners (see 8.1.2 below) whose responsibility for the day- to-day maintenance of the controls applied to their asset is documented in their job descriptions and elsewhere through the Cogent ISMS .

- All risks have identified Owners (identified during the risk assessment) whose responsibility for the acceptance of the treatment of their risk and any residual risk is documented in their job descriptions and risk treatment plan (**Risk Management Methodology**).

- Each site and facility has an identified individual the department IS officer who is responsible for co-ordinating information security activities or carrying out specific processes within that site, or facility, in line with the Manual and applicable procedures. The authority of these individuals is documented in their job descriptions. The **Cogent CISO maintains** a list of the responsible department IS officers.

- Other responsibilities are identified as necessary throughout the Cogent ISMS .

- Authorisation levels are clearly defined and documented and enforce segregation of duties (see 6.1.2 below).

6.1.2 Segregation of duties

Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of organisational assets.

- As far as is practicable and possible, Cogent segregates duties and areas of responsibility.

In particular, the following functions are segregated:

Risk assessment	**Information Security Team**
Authorisation of controls	**Chief Information Security Officer (CISO)**
Change initiation	**Functional Managers**
Change Management	**Program Change Manager**
Network Management	**Network Manager**
Network Administration	**Network Manager**
IT Operations	**IT Operations Manager**
Software development	**Head of Software Development**
System testing	**System Test Manager**
Employee Administration	**HR Manager**
Asset Purchase	**Procurement Manager**
Site/Secure Area security	**Site Manager / IS Officer**
Security Audit	**IS Audit Bureau**

- Segregation of duties is built into procedures, including the requirement that that the Owner of a procedure or process cannot authorise its modification, withdrawal or release.

- Activity monitoring, audit trails and management supervision are used to support duty segregation.

6.1.3 Contact with authorities

Cogent maintains appropriate contacts with relevant authorities. The **Cogent CISO** is responsible for identifying (Procedure document **Contact with Authorities**) those authorities with whom Cogent needs to maintain contacts, to support information security incident management (section 16, below), business continuity management (section 17, below), and continuous improvement.

6.1.4 Contact with special interest groups

Cogent maintains appropriate contact with special interest groups and other specialist security forums and professional associations.

- The **Cogent CISO is** responsible, on behalf of Cogent, for identifying and joining those forums and special interest groups which s/he considers will enable him/her to effectively meet the responsibilities contained in his/her job description.

- The **Cogent CISO is** required to ensure Cogent has up-to-date information security knowledge, including about the changing malware threat environment.

- Cogent’s Information Security Incident Management procedure sees section 16 below) requires the Cogent CISO to have suitable liaison for dealing with incidents.

6.1.5 Information security in project management

Information security is addressed in project management, regardless of the type or nature of project.

- The project management methodology is in line with the Policy document **Secure Applications development Policy**.

- The **Cogent CISO,** in conjunction with the **Project Manager** is required to ensure that information security objectives are included in project objectives.
- The project is subject to an information security risk assessment at the initiation of the project, in order to identify necessary controls.

6.2 Mobile devices and teleworking

Control objective: to ensure the security of teleworking and use of mobile devices

6.2.1 Mobile device policy

A formal policy is in place and appropriate security measures have been adopted to manage the risks introduced by using mobile devices.

- Cogent **Mobile Computing Policy** covers notebook computers, palmtops, (PDAs), laptops, tablets, smart phones and mobile phones.
- Cogent provides mobile computing facilities in order to improve the productivity, flexibility, responsiveness and effectiveness of its operations. Cogent also takes appropriate steps for physical protection (**Acceptable Usage Policy**), access controls, cryptography, backups and malware protection for mobile devices and also ensures that users receive appropriate training before they are issued with mobile devices. Users are required to accept in writing (**Acceptable Usage Policy**) specific responsibilities with regard to backups, malware protection and their use of mobile devices, particularly with regard to working in unprotected environment

6.2.2 Teleworking

Cogent does not provide teleworking facilities to its employees.

7. Human Resource Security

7.1 Prior to employment

Control objective: to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

Background verification checks on all candidates for employment and contractors are carried out in line with **Personnel Security Policy** and in accordance with the laws, regulations and ethics of the Republic of India , and proportional to Cogent business requirements, the classification of the information to be accessed, and the perceived risks.

7.1.2 Terms and conditions of employment

Employees and contractors must agree and sign the terms and conditions of their employment contract, which state their and Cogent responsibility for information security.

7.2 During employment

Control objective: to ensure that employees and contractors are aware of and fulfill their information security responsibilities.

7.2.1 Management responsibilities

Management requires employees and contractors to apply security in accordance with the policies and procedures of Cogent's ISMS.

- Management ensures that employees, contractors and third parties are appropriately briefed prior to being granted access to organisational information assets (see 7.2.2 below).

- Management ensures that employees, contractors and third parties receive guidelines on security expectations (User Agreement, job descriptions and terms and conditions of employment).

- Management provides personal leadership and example in information security and ensures that Cogent policies and procedures are followed (see 18.2.1 below).

7.2.2 Information security awareness, education and training

All employees of Cogent and, where relevant, contractors receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function.

- The Head of HR is responsible for ensuring that all users receive standard information security induction and awareness training before they are allowed to access organisational information assets. This is conducted on the basis of a training needs analysis, and includes the incident reporting procedure.

- The Cogent CISO is responsible for ensuring that all users receive regular updates and alerts on information security issues as and when necessary, and that additional security- related training is made available as and when required.

- The CISO is responsible for ensuring that specialised information security staff receive appropriate specialist training in line with their job requirements.

7.2.3 Disciplinary process

Cogent has a formal and communicated disciplinary process for employees who have committed an information security breach.
Breaches of Cogent ISMS may be treated as misconduct in terms of Cogent disciplinary policy and serious breaches may lead to dismissal.

7.3 Termination and change of employment

Control objective: to protect the organisation's interests as part of the process of changing or terminating employment

7.3.1 Termination or change of employment responsibilities

Information security responsibilities and duties that remain valid after termination or change of employment are defined, communicated to the employee or contractor, and enforced.
Upon termination or change of employment, complete a termination checklist (**Employee Exit Clearance Form**).

8. Asset Management

8.1 Responsibility for assets

Control objective: to identify organisational assets and define appropriate protection responsibilities

8.1.1 Inventory of assets

Assets associated with information and information processing facilities are identified and inventoried, and the inventory is maintained in line with the requirements of **Asset Management Policy**.

8.1.2 Ownership of assets

All assets identified (8.1.1 above) are 'owned' by a designated individual or part of Cogent and details of the Owner are identified on the asset inventory in line with **Asset Management Policy**.

8.1.3 Acceptable use of assets

Rules for the acceptable use of information and assets associated with information and information processing facilities have been identified, documented and implemented.

- The **Head of HR and Manager/Executive** (generic/line) is responsible for ensuring that all users sign User Agreements (see section 9.2 below), which set out requirements for acceptable use of information assets and in which they also explicitly accept Cogent Internet **Acceptable Use Policy**.

- These User Agreements (see section 9.2 below) also explicitly accept Cogent Rules for:

  - Use of E-mail (**Acceptable Usage Policy**).

  - The **Cogent CISO** is responsible for monitoring compliance with the **Acceptable Usage Policy**.

  - Guidelines for the use of mobile devices are included in the 'mobile on the road' annex to the User Agreement (see sections 9.2 below and 6.2 above) for users issued with such devices.

8.1.4 Return of assets

All employees and contractors are required to return all organisational assets in their possession upon termination of their employment, contract or agreement.

Upon termination of employment, complete an **Employee Exit Clearance Form** to confirm that assets have been returned.

8.2 Information classification

Control objective: to ensure that information receives an appropriate level of protection in accordance with its importance to the organisation

8.2.1 Classification of information

Information has been classified in terms of value, legal requirements, criticality and sensitivity to unauthorised disclosure or modification.

Cogent has developed guidelines for information classification, which are suited to business needs (including legality, value, criticality and sensitivity) to both restrict and share information, and to the business impacts associated with those needs, and these are contained in the Procedure document **Asset Management Procedure**.

8.2.2 Labelling of information

An appropriate set of procedures for information labelling has been developed and implemented in accordance with the classification scheme adopted by Cogent and this is set out in the Procedure document **Asset Management Procedure**.

8.2.3 Handling of assets

Procedures for handling assets have been developed and implemented in accordance with the information classification scheme adopted by Cogent, and this is set out in the Procedure document **Asset Management Procedure**.

8.3 Media handling

Control objective: to prevent unauthorised disclosure, modification, removal or destruction of information stored on media.

8.3.1 Management of removable media

Procedure document **Asset Management Procedure** identifies the controls for the management of removable media in accordance with the information classification scheme laid out in **Asset Management Methodology**.

8.3.2 Disposal of media

Media are disposed of securely and safely when no longer required, in line with the **Asset Management Procedure**.

8.3.3 Physical media transfer

The **Asset Management Procedure** sets out how Cogent ensures that media are protected against unauthorised access, misuse or corruption during transportation.

9. Access Control

9.1 Business requirements of access control

Control objective: to limit access to information processing facilities

9.1.1 Access control policy

An access control policy has been established, documented in the Policy document **Access Control Policy**, and is reviewed when required in the light of business and information security needs.

9.1.2 Access to networks and network services

Cogent policy (in Policy document **Access Control Policy**) is that users are only provided with access to the network and network services that they have been specifically authorised to use.

9.2 User access management

Control objective: to ensure authorised user access and to prevent unauthorised access to systems and services

9.2.1 User registration and de-registration

There is a formal user registration and de-registration policy (**Access Control Policy**) governing assignment of access rights.

9.2.2 User access provisioning

A formal user access provisioning policy (**Access Control Policy**) has been implemented to assign or revoke access rights for all user types to all systems and services.

9.2.3 Management of privileged access rights

The allocation and use of privileged access rights is restricted and controlled through a formal management process as set out in the Policy document **Access Control Policy**.

9.2.4 Management of secret authentication information of users

The allocation of secret authentication information is controlled through a formal management process as set out in the Policy document **Access Control Policy**.

9.2.5 Review of user access rights

Asset owners review users' access rights at regular intervals using the formal process as set out in the Policy document **Access Control Policy**.

9.2.6 Removal or adjustment of access rights

The access rights of all employees and contractors to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.

Upon termination or change of employment, complete a termination checklist (Records document **Employee Exit Clearance Form**) to confirm that all access rights have been removed or adjusted.

9.3 User responsibilities

Control objective: to make users accountable for safeguarding their authentication information

9.3.1 Use of secret authentication information

Users are required (in their User Agreements Policy document **Acceptable Usage Policy**) to follow the organisation's practices in use of secret authentication information.

9.4 System and application access control

Control objective: to prevent unauthorised access to systems and applications

9.4.1 Information access restriction

Access to information and application system functions by users and support personnel is restricted in the Policy document **Acceptable Usage Policy** in accordance with the Policy document **Access Control Policy**.

9.4.2 Secure log-on procedures

Where required by the Policy document **Access Control Policy**, access to systems and applications is controlled by the secure log-on procedures set out in the procedure document **Secure Log-on Procedure**.

9.4.3 Password management system

The interactive password management system set out in Policy document **Access Control Policy** ensures quality passwords.

9.4.4 Use of privileged utility programs

The use of utility programs that might be capable of overriding system and application controls is restricted and controlled as specified in Policy document **Access Control Policy**.

9.4.5 Access control to program source code

Access to program source code is restricted in line with the Policy document **Access Control Policy**.

10. Cryptography

10.1 Cryptographic controls

Control objective: to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Policy on the use of cryptographic controls

Cogent has a policy on its use of cryptographic controls for protection of its information, as set out in 10.1.1.1 below.

Cogent applies cryptographic controls to secure its confidential communications and information carried beyond its secure logical perimeter, to secure connections from beyond its logical perimeter, and to secure its business (as required in the Policy document **Secure Application Development Policy**).

The Cogent CISO is responsible for maintaining required cryptographic controls, which sets out, for each situation in which cryptographic controls are required under this policy, the type and length of the encryption algorithm required, and identifies the precise instructions required to use that cryptographic control. They are responsible for key management and [key generation] as set out in the Policy document **Encryption and Key Management Policy**. Each asset Owner, whose information asset falls within the scope of this policy, is responsible for ensuring that the required cryptographic control is applied. The Manager/Executive (generic/line) is responsible for configuration of devices as required by this policy.

10.1.2 Key management

Cogent has a policy on the use, protection and lifetime of cryptographic keys, as documented in the Policy document **Encryption and Key Management Policy**, which supports Cogent use of cryptographic techniques.

11. Physical and Environmental Security

11.1 Secure areas

Control objective: to prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities

11.1.1 Physical security perimeter

Cogent uses security perimeters to protect areas that contain sensitive or critical information and information processing facilities.

- All Cogent sites have physical security perimeters. The minimum specification checklist for the physical security perimeter is in the Policy document **Physical Security Policy and** the Premises Security Manager ensures that each site is checked on a biannual basis.

- The Site Manager of each organizational site is responsible for maintaining that site's secure perimeter.

- Cogent central information processing facilities are within secure areas **server room/communication**s room, each of which have Owners (see section 8.1.2 above) that are themselves within a site's secure perimeter.

- The Cogent CISO has a site map for each site or secure area, together with a current security checklist the Policy document **Physical Security Policy** that identifies the current state of conformity to the requirements in that checklist.

11.1.2 Physical entry controls

Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

- A risk assessment (see section 4.4 above) is used to determine the type of entry controls that might be required for secure areas and these are implemented in line with the requirements of the Policy document **Physical Security Policy**.
- The Site Managers are responsible for maintaining required physical entry controls.

11.1.3 Securing offices, rooms and facilities

Cogent has designed and applied physical security for offices, rooms and facilities. Cogent conducts risk assessments in line with Methodology Document **Risk Management Methodology** of individual offices, rooms and facilities that contain confidential or high risk information assets to identify the controls that might be necessary to secure them. These are implemented in line with the Policy document **Physical Security Policy**. There are no sites where confidential information processing facilities are shared with a third party organisation, other than under the terms of a contract (see section 15.1.2 below).

11.1.4 Protecting against external and environmental threats

Cogent has designed and applied physical protection against damage from natural disasters, malicious attack or accidents.

Cogent has assessed the risk of external and environmental threats and has applied controls that are included in the Policy document **Physical Security Policy** or that are part of the Business Continuity Management framework (see section 17).

11.1.5 Working in secure areas

Cogent has designed and applied procedures for working in secure areas and these are contained in the Policy document **Physical Security Policy**.

11.1.6 Delivery and loading areas

Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorised access.

Cogent controls for delivery and loading areas are detailed in the Policy document **Physical Security Policy.**

11.2 Equipment

Control objective: to prevent loss, damage, theft or compromise of assets and interruption to the organisation’s operations

11.2.1 Equipment siting and protection

Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

The Site Manager is responsible for implementing the requirements of the Policy document **Physical Security Policy**, which include this control.

11.2.2 Supporting utilities

Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.
The Site Manager is responsible for implementing the requirements of the Policy document **Physical Security Policy**, which include this control.

11.2.3 Cabling security

Power and telecommunications cabling carrying data or supporting information services is protected from interception, interference or damage.

The Site Manager is responsible for implementing the requirements of the Policy document **Physical Security Policy**, which include this control.

11.2.4 Equipment maintenance

Equipment is correctly maintained to ensure its continued availability and integrity.
The Site Manager is responsible for implementing the requirements of the Policy document **Physical Security Policy**, which include this control.

11.2.5 Removal of assets

Equipment, information or software may not be taken off-site without prior authorisation as required by the Methodology document **Asset Management Methodology**.

11.2.6 Security of equipment and assets off-premises

Security is applied to off-site equipment and assets taking into account the different risks of working outside Cogent premises.

- Users of mobile equipment are required, as part of their User Agreements (see 9.1 above), to provide appropriate physical security for equipment when off-site and to ensure that manufacturer’s instructions for protecting equipment are followed.
- Home working is subject to specific controls, in line with 6.2.2 above.
- The Finance Director (CFO) is responsible for ensuring that the Organisation’s insurance specifically provides cover against loss of or damage to mobile devices off- site.

11.2.7 Secure disposal or re-use of equipment

All items of equipment containing storage media are checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

11.2.8 Unattended user equipment

Users are required to ensure that any unattended equipment is appropriately protected as per the Policy document **Acceptable Usage Policy**.

11.2.9 Clear desk and clear screen policy

Cogent has adopted a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities, and the requirement for compliance with this policy is set out in the Policy document **Clear Desk Clear Screen Policy**.

12. Operations Security

12.1 Operational procedures and responsibilities

Control objective: to ensure correct and secure operation of information processing facilities

12.1.1 Documented operating procedures

Operating procedures have been documented, are maintained and are made available to all users who need them.

The Cogent CISO is responsible for documenting all the IT working procedures for system activities related to information processing and communications facilities. The procedures required by Cogent are listed in the **Document**

12.1.2 Change management

Changes to Cogent , business processes, information processing facilities and systems that affect information security are controlled.

The Program Control Manager is responsible for ensuring that all requests for significant non-routine changes to organisational information processing facilities are managed in line with the Procedure document **Change Control Procedure** and section 14.2 below is also relevant.

12.1.3 Capacity management

Policy document **Communication and Operations Management Policy** sets out Cogent approach to ensuring that the use of resources is monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

12.1.4 Separation of development, test and operational environments

Development, testing and operational environments are separated to reduce the risks of unauthorised access or changes to the operational environment.

Cogent requirements for separate development, test and operational facilities, and its rules for their use and for the transfer of software to the operational environment are documented in the Policy document **Secure Application Development Policy**.

12.2 Protection from malware

Control objective: to ensure that information and information processing facilities are protected against malware.

12.2.1 Controls against malware

Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures have been implemented, and user awareness programmes incorporate this.

12.3 Backup

Control Objective: to protect against loss of data

12.3.1 Information backup

Back-up copies of information, software and system images are taken and tested regularly in accordance with the agreed policy document **Data Backup Policy** below.

Cogent policy is that it acts to maintain the integrity and availability of information and information processing facilities by establishing criteria and routine procedures (in **Communications and Operational Management Policy**) to ensure that all Cogent information assets are backed up and that there are tested procedures (see section 17 below) for restoring them within an adequate time frame.

12.4 Logging and monitoring

Control objective: to record events and generate evidence.

12.4.1 Event Logging

Event logs recording user activities, exceptions, faults and information security events are produced and kept, in line with the Policy document **System Usage Monitoring Policy**, for a period specified in Procedure document **Retention of Records Procedure**, and regularly reviewed to assist in future investigations and access control monitoring.

12.4.2 Protection of log information

Logging facilities and log information are protected against tampering and unauthorised access, as required by the Policy document **System Usage Monitoring Policy**.

12.4.3 Administrator and operator logs

System administrator and system operator activities are logged and the logs are protected, as required by the Policy document **System Usage Monitoring Policy**.

12.4.4 Clock synchronisation

The clocks of all relevant information processing systems within Cogent or security domain are synchronised to a single reference time source, as specified in the Policy document **System Usage Monitoring Policy**.

12.5 Control of operational software

Control objective: to ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

The installation of software on operational systems is controlled by the Policy document **Communications and Operations Management Policy**.

12.6 Technical vulnerability management

Control objective: to prevent exploitation of technical vulnerabilities

12.6.1 Management of technical vulnerabilities

Timely information about technical vulnerabilities of information systems used by Cogent is obtained, Cogent exposure to those vulnerabilities evaluated, and the Policy document **Vulnerability and Penetration Testing Policy** sets out the measures taken to address the associated risks.

12.6.2 Restrictions on software installation

Rules have been established governing the installation of software by users, as described below.

- Using externally evaluated and certificated products
- Installation and updating third party commercial software is described in the Policy document **Communications and Operations Management Policy**.
- Malware, that might cause covert channels, is controlled through the anti-malware software (see 12.2 above) and User Agreements (see 9.2 and 9.3 above).

12.7 Information systems audit considerations

Control objective: to minimise the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

Audit requirements and activities involving checks on operational systems are carefully planned as set out in the Procedure document **Internal Audit Procedure** and agreed with appropriate management to minimize the risk of disruptions to business processes.

13. Communications Security

13.1 Network security management

Control objective: to ensure the protection of information in networks and its supporting information processing facilities

13.1.1 Network controls

Networks are managed and controlled as set out in the Policy document **Communications and Operations Management Policy**, in order to protect information in systems and applications.

13.1.2 Security of network services

Security mechanisms, service levels and management requirements of all network services have been identified and included in any/the network services agreements, whether those services are provided in-house or outsourced and are managed in line with the Policy document **Communications and Operations Management Policy**

13.1.3 Segregation in networks

Groups of information services, users and information systems are segregated on the network(s) in line with the requirements of the Policy document **Communications and Operations Management Policy**.

13.2 Information transfer

Control objective: to maintain the security of information transferred within the organisation and with any external entities.

13.2.1 Information transfer policies and procedures

Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities.

- Cogent **Acceptable Usage Policy**, including internet and e-mail usage rules, its information classification procedures (**Asset Management Procedure**), its anti-malware policy (**Anti Malware Policy**) and related procedures, and the technological controls implemented as required in all those procedures, protect exchanges of information from interception, unauthorised copying, modification, destruction or misrouting.

- The wireless user's addendum to the standard User Agreement (see section 9.1 of this Manual) sets out how wireless communication is protected.

- The mobile phone user's addendum to the standard User Agreement (see section 9.1 of this Manual) sets out how mobile voice communication is protected.

- Cogent has a procedure (Policy document **Communications and Operations Management Policy**) for secure voice communication at all its sites].

- Cogent use of cryptographic techniques is controlled under section 10.1 above.
- Cogent has procedures for handling, retention and disposal of information and related media.

13.2.2 Agreements on information transfer

Agreements are established in line with the Policy document **Communications and Operations Management** for the transfer of information, and address the secure transfer of business information between Cogent and external parties.

13.2.3 Electronic messaging

Information involved in electronic messaging is appropriately protected.

- Policy document **Acceptable Usage Policy** sets out Cogent rules on e-mail usage, and Procedure document **Asset Management Procedure** sets out security requirements related to information classification, encryption and digital signatures and users are trained on correct use of e-mail, including the requirement to verify that e-mail addresses are correct prior to despatch.

- The Manager/Executive (generic/line) is responsible for ensuring that Cogent e-mail system is set up and configured in line with the policies and procedures, which were drawn up to document the controls identified in the e-mail risk assessment.

- The Manager/Executive (generic/line) is responsible for Cogent web mail service and for its protection by a firewall configured according to necessary request forms and for ensuring that it is only accessible to authorised and authenticated users by means of a secure channel, the configuration of which is in line with the policies and procedures.

- The Business Continuity Manager is responsible for business continuity plans in respect of the e-mail systems, (see section 17 below).

- Instant messaging systems require specific authorisation from the Manager/Executive (generic/line). Their configuration is subject to the policies and procedures and the user requirements are set out in the User Agreement.

13.2.4 Confidentiality or non-disclosure agreements

A confidentiality and non-disclosure agreement (Procedure document **Confidentiality Agreements Procedure**) reflecting Cogent requirements for the handling of information is in place (also see 7.1.2 above) and is reviewed regularly

14. System Acquisition, Development and Maintenance

14.1 Security requirements of information systems

Control objective: to ensure that information security is an integral part of information systems across the entire lifecycle. This includes the requirements for information systems which provide services over public networks.

14.1.1 Security requirements analysis and specification

Statements of information security requirements are included in the requirements for new information systems, or enhancements to existing information systems.

- Cogent carries out a risk assessment (in line with Procedure document **Risk Management Procedure**) at the requirements stage of specifying any new information systems, or enhancements to existing systems (irrespective of whether they will be bespoke systems or commercial off the shelf systems). Required controls are identified and the Procurement Manager is responsible for ensuring that these controls are integrated into the purchase decision, specification and purchase contract. The Cogent CISO is responsible for ensuring that required manual controls are designed and implemented.

- Application controls that ensure correct processing are also (where appropriate) considered at the design stage.

- Software is subject to testing and formal approval in line with the Policy document **Secure Application Development Policy**; non-compliant products are not accepted.

14.1.2 Securing application services on public networks

Information involved in application services passing over public networks is protected from fraudulent activity, contract dispute and unauthorised disclosure and modification, as set out in the Policy document **Secure Application Development Policy**.

14.1.3 Protecting application services transactions

Information involved in application service transactions is protected in line with the Policy document **Secure Application Development Policy** to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

14.2 Security in development and support processes

Control objective: to ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Secure development policy

Rules for the development of software and systems have been established and documented in the Policy document **Secure Application Development Policy**, and must be applied to developments within the organisation and contracted development by third parties.

14.2.2 System change control procedures

Changes to systems within the development lifecycle are controlled by the use of the formal change control procedures set out in the Procedure document **Change Control Procedure**

14.2.3 Technical review of applications after operating platform changes

When operating platforms are changed, business critical applications are reviewed and tested in line with the Policy document **Secure Application Development Policy** to ensure there is no adverse impact on organisational operations or security.

14.2.4 Restrictions on changes to software packages

Cogent does not seek bespoke modifications to commercial software packages

14.2.5 Secure system engineering principles

Principles for engineering secure systems have been established in the Policy document **Secure Application Development Policy**, and are to be applied to any information system implementations

14.2.6 Secure development environment

Cogent has established a procedure for appropriately protected secure development environments for system development and integration efforts that cover the entire system development lifecycle, and this is in line with the Policy document **Communications and Operations Management Policy**.

14.2.7 Outsourced software development

Rules for the outsourced development of software and systems have been established and documented in the Policy document **Secure Application Development Policy**, and must be applied to outsourced software developments by third parties.

14.2.8 System security testing

Security functionality is tested during development, as described in the Policy document **Secure Application Development Policy**

14.2.9 System acceptance

Acceptance criteria for new information systems, upgrades and new versions have been established and suitable tests of the system(s) are carried out during development and prior to acceptance, all as specified in the Policy document **Communications and Operations Management Policy**.

14.3 Test Data

Control objective: to ensure the protection of data used for testing.

14.3.1 Protection of test data

Test data is selected carefully, protected and controlled in line with the Policy document **Communications and Operations Management Policy**.

15. Supplier Relationships

15.1 Information security in supplier relationships

Control objective: to ensure protection of the organisation's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Cogent agrees information security requirements with suppliers for mitigating the risks associated with access to Cogent information assets.

- Cogent has a defined policy (**Third Party Services Policy**) governing information security in supplier relationships.
- Cogent has a defined process (**Third Party Services Policy**) for managing third party service contracts.

15.1.2 Addressing security in third party agreements

Agreements with suppliers account for information security involving suppliers accessing, processing, storing, communicating or providing IT infrastructure components, as required in the Policy document **Third Party Services Policy** , and suppliers are not allowed to access Cogent information assets until such an agreement has been signed.

Where a supplier has a standard agreement and no provision to vary it to meet a client's requirement, the supplier's standard clauses are assessed against Cogent requirements and the risk associated with the gap is assessed before deciding whether or not to proceed with the offered terms. Where there is a significant variation between the requirements and what is offered, the General Manager (GM)'s approval to proceed with the provider is required.

15.1.3 Information and communication technology supply chain

Agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.

15.2 Supplier service delivery management

Control objective: to maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Monitoring and review of supplier services

Cogent regularly monitors, reviews and audits supplier service delivery, in line with the Policy document **Third Party Services Policy**.

15.2.2 Managing changes to supplier services

Cogent manages changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, taking account of the criticality of business information systems and processes involved and re- assessment of risks, and the procedures for doing this are contained in the Policy document **Third Party Services Policy**.

16. Information Security Incident Management

16.1 Management of information security incidents and improvements

Control objective: to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 Responsibilities and procedures

Management responsibilities and procedures have been established in the Procedure document **Incident Management Procedure** to ensure a quick, effective and orderly response to information security incidents that ensures appropriate corrective or preventative actions, restores normal operations as quickly as possible, and ensures that improvement opportunities are identified and acted upon.

16.1.2 Reporting information security events

Information security events must be reported to the **Cogent CISO** as quickly as possible, as set out in the Procedure document **Incident Management Procedure**

16.1.3 Reporting information security weaknesses

All employees and contractors using information systems and services are required by the Procedure document **Incident Management Procedure** to note and report to the **Cogent CISO** any observed or suspected weaknesses in systems or services

16.1.4 Assessment of and decision on information security events

Information security events are assessed in order to determine whether they are classified as information security incidents, in line with the Procedure document **Incident Management Procedure**

16.1.5 Response to information security incidents

Information security incidents are responded to in accordance with the Procedure document **Incident Management Procedure**

16.1.6 Learning from information security incidents

Knowledge gained from analysing and resolving information security incidents is to be used to reduce the likelihood or impact of future incidents, as described in the Procedure document **Incident Management Procedure**

16.1.7 Collection of evidence

In all information security incidents, irrespective of whether or not a follow-up action against a person or organisation involves legal action (either civil or criminal), evidence is collected, retained and presented as set out in the Procedure document **Incident Management Procedure** to conform to the rules for evidence laid down within the legal jurisdiction(s) of the Republic of India .

17. Information Security Aspects of Business Continuity Management

17.1 Information security continuity

Control objective: information security continuity is embedded in the organisation's business continuity management systems.

17.1.1 Planning information security continuity

Cogent has determined its requirements for information security and the continuity of information security management in adverse situations, a described in the single framework (as described in the Policy document **Information Security Continuity Policy**).

17.1.2 Implementing information security continuity

Cogent has established and implemented processes, procedures and controls to ensure the required level of continuity for information security during adverse situations, as described in the Policy document **Information Security Continuity Policy**.

17.1.3 Verify, review and evaluate information security continuity

Cogent verifies the established and implemented information security controls at regular intervals (as described in the Policy document **Information Security Continuity Policy**) in order to ensure that they are effective during adverse situations.

17.2 Redundancies

Control objective: to ensure availability of information processing facilities

17.2.1 Availability of information processing facilities

Information processing facilities are implemented with redundancy sufficient to meet availability requirements, as described in the Policy document **Information Security Continuity Policy**.

18. Compliance

18.1 Compliance with legal and contractual requirements

Control objective: to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

All relevant legislative, statutory, regulatory and contractual requirements and Cogent approach to meet these requirements have been explicitly defined, documented and are kept up to date for each information system and Cogent .

- All legislative, contractual, statutory and regulatory requirements that apply to Cogent and to its information assets are identified by Cogent CISO in a compliance database.
- The Cogent CISO is responsible for creating and maintaining the multi-jurisdictional database (in line with the Policy document **Compliance Policy**) of Cogent statutory and regulatory information/data and computer-related compliance requirements. The controls and responsibilities necessary to meet these compliance requirements are also identified in this schedule.

18.1.2 Intellectual property rights

Appropriate procedures have been implemented to ensure compliance with legislative, regulatory and contractual requirements relating to intellectual property rights and on the use of proprietary software products.

- Cogent has adopted a policy on intellectual property rights compliance which is set out in the Policy document **Software Copyright Policy**. This policy is prominently displayed near all digital copying equipment and elsewhere, as appropriate.
- Cogent procedures to implement this policy are contained in the Policy document **Software Copyright Policy**.

18.1.3 Protection of records

Cogent procedure, set out in the Policy document **Privacy Policy**, protects records from loss, destruction, falsification and unauthorised access, in accordance with legislatory, regulatory, contractual and business requirements.

18.1.4 Privacy and protection of personally identifiable information

Cogent ensures the privacy and protection of personally identifiable information as required in relevant legislation and regulation.

- Cogent Data Protection and Privacy policy is set out in the Policy document **Privacy Policy**.
- Cogent has implemented specific technical measures to protect personal information.

18.1.5 Regulation of cryptographic controls

Cryptographic controls are used in compliance with all relevant agreements, legislation and regulations, as set out in the Policy document **Encryption and Key Management Policy**.

18.2 Information security reviews

Control objective: to ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

18.2.1 Independent review of information security

Cogent approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) is independently reviewed at planned intervals, and when significant changes to the security implementation occur.

- The **CISO** is responsible for organizing independent audits of the Cogent ISMS .
  - Where necessary, the **CISO** in conjunction with the **Cogent CISO** engages expert technical external assistance. The audit procedures are contained in the Procedure document **Internal Audit Procedure** and section 12.7 of this Manual is also applicable.
- The Cogent ISMS is also subject to periodic reviews by external compliance auditors.
- Risk assessments are independently reviewed annually to ensure that they are still complete and up-to-date.

18.2.2 Compliance with security policies and standards

Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

- Manager/Executive (generic/line) are required, under their job descriptions, to carry out monthly checks to ensure that all security procedures and work instructions within their area of responsibility are being carried out, to identify shortfalls and to take action to ensure that shortfalls are immediately corrected. This action should involve identification of the causes of the non-compliance, an evaluation of the need for action to ensure non-recurrence of the shortfall, a determination of the appropriate action, followed by a review of the action to ensure that it has achieved its objectives. This follows Cogent continual improvement approach.

- Managers are required to document these reviews in accordance with the Policy document **Compliance Policy** as well as the actions required, and responsibilities and timeframes, in the case of shortfalls.
- These management reviews and any actions arising must be reported in accordance with the Policy document **Compliance Policy** to the independent reviewers.

18.2.3 Technical compliance review

Information systems are regularly reviewed and tested for compliance with Cogent information security policies and standards, as set out in the Policy document **Compliance Policy**.

End of Document